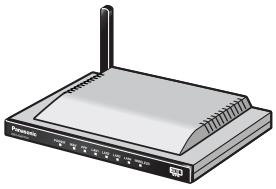
Panasonic®



Operating Instructions
Version 1.1

Network Camera Management System

Model No. BB-HGW700A

Please read this manual before using and save this manual for your future reference.

Panasonic Web Site: http://www.panasonic.com
for customers in the USA or Puerto Rico

Introduction

Thank you for purchasing the Panasonic Network Camera Management System.

Before using

Please read the Important Safety Instructions on page 4 before using.
Read and understand all instructions.

For Operation Assistance

- Call **1-800-272-7033**
- See the Panasonic web site **http://www.panasonic.com**

System Requirements

Item	Description
Operating System (IPv6)	Windows® XP
Operating System (IPv4)	Windows® XP, Windows® 2000, Windows® Me, Windows® 98SE
Interface	10/100 Mbps network card installed
Memory	Over 64 MB
Protocol	TCP/IP protocol
Web Browser	Internet Explorer 6.0 or later

Note

If you have any inquiries regarding your PC, contact your PC dealer.

Compatible cameras (Customer-provided) : (as of Mar. 2005)

Indoor type
KX-HCM8
KX-HCM10
KX-HCM250
KX-HCM280
BB-HCM311A
BL-C10A
BL-C30A
BB-HCM381A

Outdoor type
KX-HCM230
KX-HCM270
BB-HCM331A
BB-HCM371A

Abbreviations

- UPnP is the abbreviation for Universal Plug and Play.
- CATV modems and ADSL modems are referred to as modems in this manual.
- Network cameras are referred to as cameras in this manual.

Trademarks

- Microsoft, MSN, Windows and DirectX are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.
- Screen shots reprinted with permission from Microsoft Corporation.
- All other trademarks identified herein are the property of their respective owners.

Network Camera Management System Memo

Attach your purchase receipt here.

For your future reference

Date of purchase

Serial Number MAC Address

Name and address of dealer

IMPORTANT SAFETY INSTRUCTIONS

When using this product, basic safety precautions should always be followed to reduce the risk of fire, electric shock, or personal injury.

1. Read and understand all instructions.
2. Keep these instructions.
3. Heed all warnings.
4. Follow all instructions.
5. Do not install this product near any heat sources such as radiators, heat registers, stoves, or other apparatus (including amplifiers) that produce heat.
6. Protect the AC adaptor cord and AC cord from being walked on or pinched particularly at plugs, convenience receptacles, and the point where they exit from this product.
7. The AC cord is used as the main disconnect device, ensure that the AC outlet is located/installed near the product and is easily accessible.
8. Use only the included Panasonic AC adaptor and AC cord.
9. The AC adaptor must remain connected at all times. (It is normal for the adaptor to feel warm during use.)
10. To prevent the risk of fire or electrical shock, do not expose this product to rain or any type of moisture.
11. Do not touch the product or the AC adaptor and AC cord during lightning storms.
12. Unplug this product when unused for a long period of time.
13. Refer all servicing to qualified service personnel. Servicing is required when this product has been damaged in any way, such as when the AC adaptor, AC cord or plug is damaged, this product does not operate normally, or it has been dropped.

SAVE THESE INSTRUCTIONS

Table of Contents

1 Product Introduction 7
1.1 Main Features 7
1.2 Included Accessories 8
1.3 Feature Locations 9
1.3.1 Front View 9
1.3.2 Rear View 9
1.3.3 Indicators 10
2 Accessing This Product 11
2.1 Functions 11
2.1.1 Top Page 11
2.1.2 Setup 13
2.1.3 IPv6 Setup 16
2.1.4 Camera Portal 17
3 Functions 22
3.1 Using the Functions 22
3.1.1 Registering ISPs 22
3.1.2 Registering IPv6 ISPs 30
3.1.3 Confirming Connection to the Internet 37
3.1.4 Managing the Connection Mode 38
3.1.5 Using Camera 40
3.1.6 Registering a Camera Automatically 42
3.1.7 Using Wireless 48
3.1.8 Using DynamicDNS 56
3.2 Using Advanced Setup 60
3.2.1 Accessing this Product from the Internet 60
3.2.2 Improving Security 66
3.2.3 Improving IPv6 Security 72
3.2.4 Using Options 77
- LAN IP Address DHCP Server 77
- PPPoE 79
- DNS Relay 80
- MTU Size 80
- Routing 81
- UPnP™ 82
- MAC Clone 84

3.2.5 Using IPv6 Options 85
- IPv6 Address(LAN) RA 85
- Link MTU size 86

- Routing 86

3.2.6 Using VPN (PPTP) 88
3.2.7 Using VPN (IPsec) 90
3.2.8 Using Applications 98
3.3 Managing This Product 101
3.3.1 Changing The Password 101
3.3.2 Updating Firmware 102
3.3.3 Saving Settings 104
3.3.4 Restarting 105
3.3.5 Initializing The Settings 105
3.3.6 Using PPPoE Connection 106
3.3.7 Using VPN (IPsec) Connection 107
3.3.8 Confirming Network Connection 108
3.4 Getting Information 109
3.4.1 Getting Network Information 109
3.4.2 Viewing Logs 112
3.4.3 Support 116
3.4.4 Help 116

4 Other Information 117

4.1 Factory Default 117
4.1.1 Factory Default 117
4.1.2 Restart 117
4.2 Disabling Pop-up Blocker 118
4.3 UPnP™ Setup on your PC 119
4.4 IPv6 Setup on your PC 124
4.4.1 Setting an IPv6 Address Using Windows XP 124
4.4.2 Re-obtaining an IPv6 Global Address 127
4.4.3 Setting a Static IPv6 Global Address. 127
4.5 PPTP Setup when Using VPN: Windows XP 128
4.6 Web Browser Setup when Using a Proxy Server 131
4.7 Checking the PC's IP Address and MAC Address 132
4.7.1 Using Windows XP/2000 132
4.7.2 Using Windows Me/98SE 133
4.8 Stabilizing the PC's IP Address 135
4.8.1 Using Windows XP/2000 136
4.8.2 Using Windows Me/98SE 138
4.9 Factory Default Settings List 140
4.10 Specifications 145

Index 149

1 Product Introduction

1.1 Main Features

This product is a Network Camera Management System with the following features:

■ IPv6 Compatible

This product is compatible with IPv6, the next generation of Internet protocol. There are a number of merits to this, such as, abundant global addresses and security improvement through using IPsec.

■ Camera Privacy Protection with VPN

This product is compatible with PPTP (IPv4) and IPsec (IPv4/IPv6) for VPN. Security is ensured by encrypting all camera and PC data connected to this product before it is sent.

■ High speed wireless LAN for IEEE 802.11b/g

802.11g has 2 modes: 1. the 802.11g only mode, and 2. the 802.11g and 802.11b simultaneous mode. Also, the wireless LAN function can be suspended.

■ High speed throughput

Maximum WAN - LAN wired connection speeds of 98 Mbps (IPv4/SmartBits), 98 Mbps (IPv6/SmartBits), and 16 Mbps (FTP[PPTP]).

■ Automatic Setup

By using this product with Panasonic's network camera (Customer-provided), the camera's automatic registration function can automatically set up wireless security (encryption WEP setup etc.) and camera network related settings. (port forwarding setup etc.)

■ Camera Portal

By using this product with Panasonic's network camera (Customer-provided), the camera portal can list up to 16 camera names and their still images on a monitoring screen. Also, the camera portal page is set up automatically.

■ Cell Phone Camera Portal

Create a portal page to access your cameras easily from a cell phone. Cameras on location can be added automatically, and remote cameras can also be added.

■ Camera Status Notification

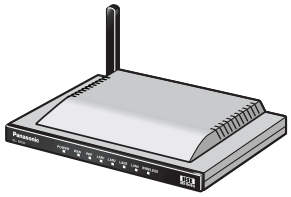
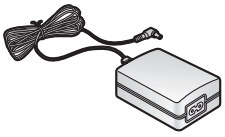
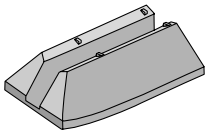
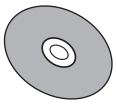
This product can send an E-mail to your PC or mobile phone, if a camera disconnection is detected.

Note

- **LAN** <Local Area Network>: A computer network limited to the immediate area, usually the same building or floor of a building. LAN IP addresses, a.k.a "local IP address" typically begin with 192.168.xxx.xxx.
- **WAN** <Wide Area Network>: A computer network that spans a relatively large geographical area and usually includes Internet access. In this manual "WAN" refers to your Local Area Network connected to this device as well as Internet access provided by your local Internet Service Provider (ISP).

1.2 Included Accessories

The following items are provided with this product. Additional pieces can be ordered by calling 1-800-332-5368.

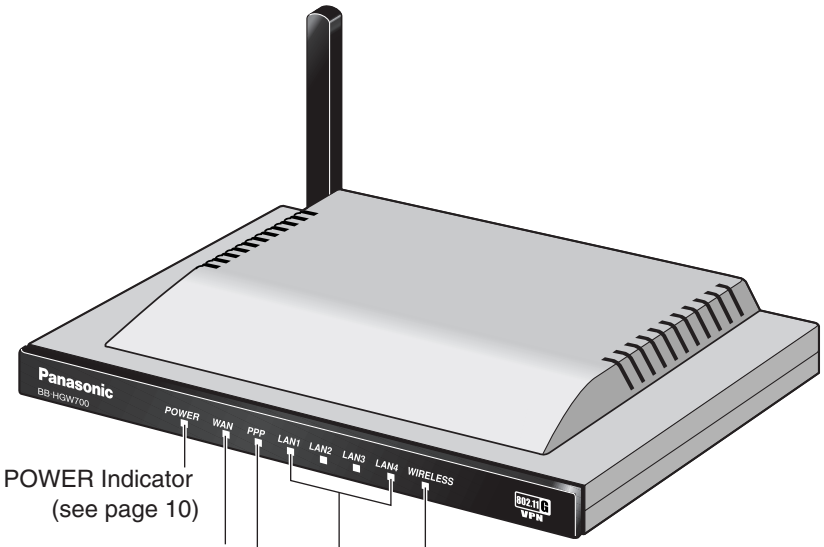
Main unit .....1 pc. 	AC adaptor.....1 pc. (Cord length: approx. 3 m (9.8 feet)) Order No. PQLV202Y 	AC cord ..... 1 pc. (Cord length: approx. 1.8 m (5.9 feet)) Order No. PSJA1069Z
Ethernet® cable (category 5 straight cable).....1 pc. (Cable length: approx. 1 m (1.1 yards)) Order No. PQJA10138Z 	Stand ..... 1 pc. Order No. PQYLHGW502 	CD-ROM..... 1 pc. (Operating Instructions etc.) Order No. PSQX3487XCD 
• Installation/Troubleshooting - 1 pc. • Warranty - 1 pc.		

Accessories to be Provided by Customer

- Ethernet Cable (category 5 straight cable) - 1 pc.
- Network Camera
- PC

1.3 Feature Locations

1.3.1 Front View



POWER Indicator
(see page 10)

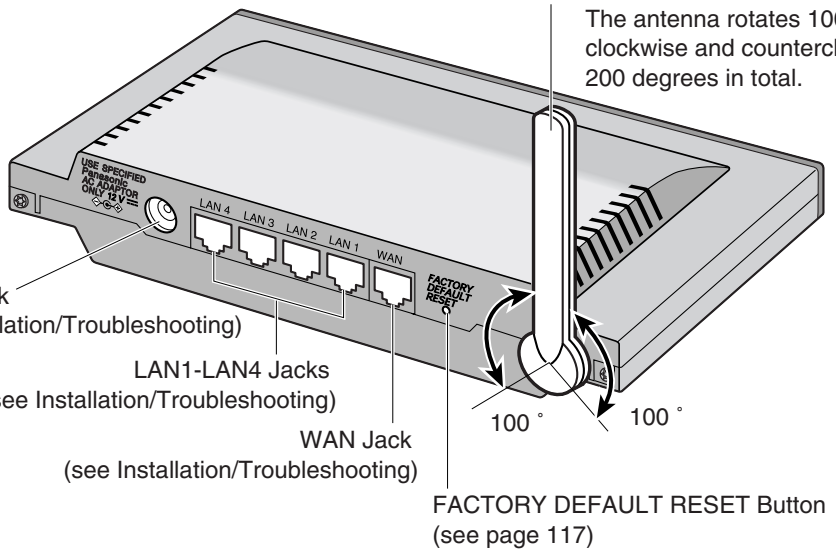
WAN Indicator
(see page 10)

PPPoE Indicator
(see page 10)

LAN1-LAN4 Indicators
(see page 10)

WIRELESS Indicator
(see page 10)

1.3.2 Rear View



Diversity Antenna
The antenna rotates 100 degrees clockwise and counterclockwise, 200 degrees in total.

DC IN Jack
(see Installation/Troubleshooting)

LAN1-LAN4 Jacks
(see Installation/Troubleshooting)

WAN Jack
(see Installation/Troubleshooting)

100 °

100 °

FACTORY DEFAULT RESET Button
(see page 117)

1.3.3 Indicators

Indicators	Light Color	Description
POWER	Green	This product is turned on.
	Red (Blinking)	There is a problem with this product. Remove the AC cord from the outlet, and insert again.
	Green (Blinking)	The firmware is damaged. Download a firmware file (see page 31 - Installation/ Troubleshooting).
WAN	Green	This product is successfully connected to a modem or an Ethernet hub etc.
	Green (Blinking)	This product is connected and sending or receiving data.
LAN1—LAN4	Green	This product is successfully connected to a PC or Ethernet hub.
	Green (Blinking)	This product is sending or receiving data.
WIRELESS	Green	This product is successfully connected to a wireless device.
	Green (Blinking)	This product is sending or receiving data in a wireless LAN.
	Orange	This product is not connected to a wireless device.
	No light	The communication mode is set to disabled, and the wireless LAN is not being used. (see page 48)
PPPoE	Green (Blinking)	PPPoE connection is in progress.
	Green	PPPoE connection is complete.
	Orange	A PPPoE authentication error has occurred.

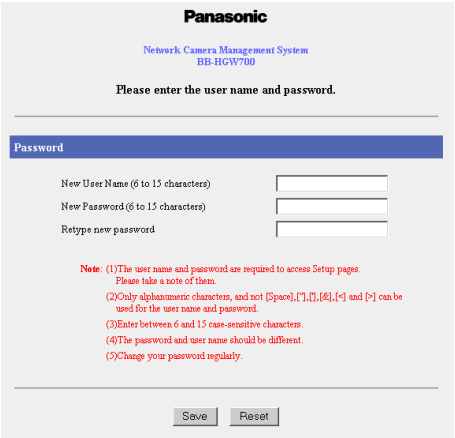
2 Accessing This Product

2.1 Functions

2.1.1 Top Page

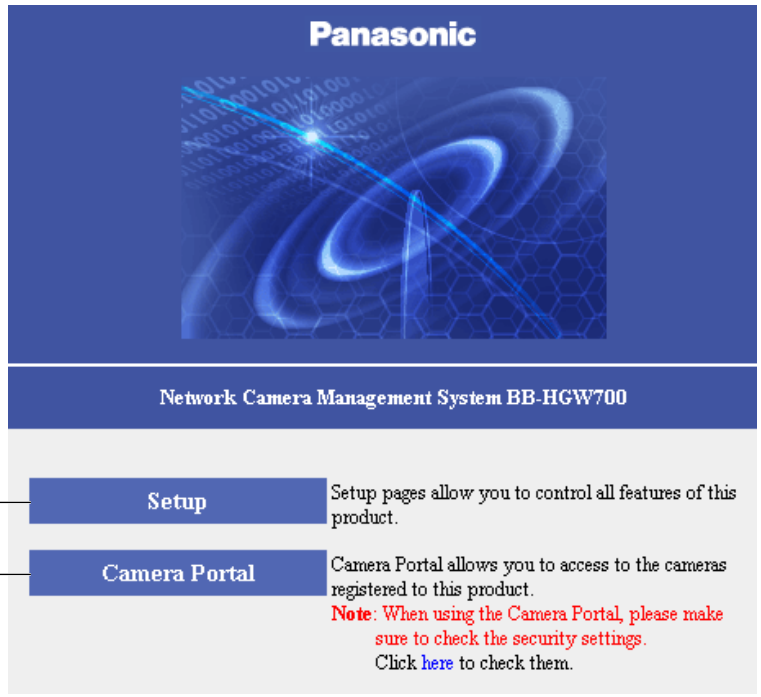
The top page allows you to select the Setup page or Camera Portal page.
The Camera Portal page displays the images of the camera connected to this product.

1. Enter "**http://bbhgw.webpage:8080**" into the web browser's address bar. (The default port number is 8080.)
- The user name and password window is displayed.


Panasonic
Network Camera Management System
BB-HGW700
Please enter the user name and password.
Password
New User Name (6 to 15 characters)
New Password (6 to 15 characters)
Retype new password
Note: (1)The user name and password are required to access Setup pages. Please take a note of them.
(2)Only alphanumeric characters, and not [Space],["],[\],[&],[<] and [>] can be used for the user name and password.
(3)Enter between 6 and 15 case-sensitive characters.
(4)The password and user name should be different.
(5)Change your password regularly.
Save
Reset

2. Enter New User Name, New Password, and Retype New Password and click [Save].
- The top page is displayed.

Notes
- It is important to always use your user name and password for authentication when using this product.
- Access information (user name/password), this product's setup information, application setup information, logs and other system management information is the responsibility of the customer. Access to this information should be limited to users or user groups, and third parties should not be allowed to refer to, modify, delete or copy this information. Information such as user name, password, setup and management information should be kept confidential.


Panasonic
Network Camera Management System BB-HGW700
Setup
Setup pages allow you to control all features of this product.
Camera Portal
Camera Portal allows you to access to the cameras registered to this product.
Note: When using the Camera Portal, please make sure to check the security settings.
Click here to check them.

Setup (see page 13)

Camera Portal (see page 17)

Notes

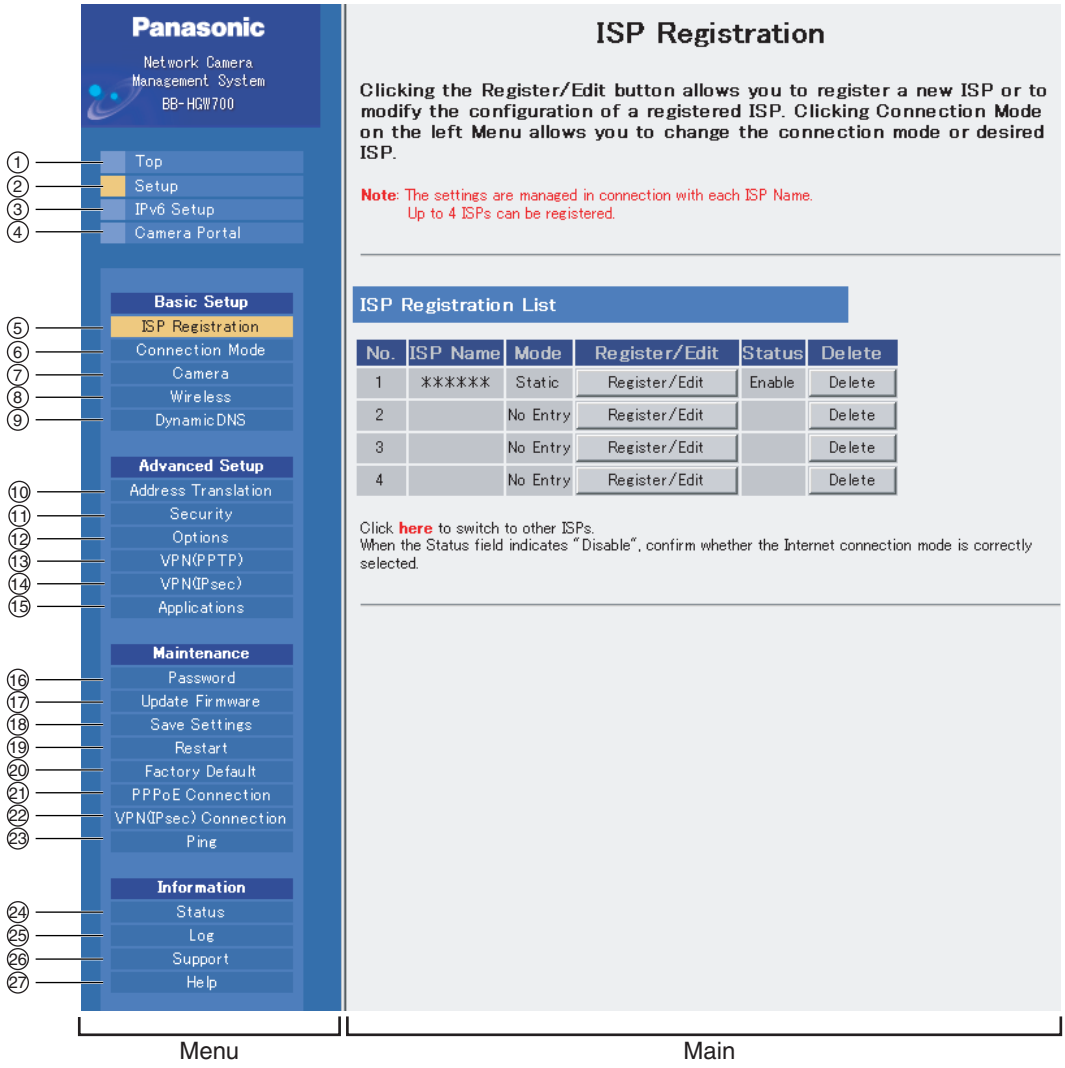
- In the default settings, it is possible to display the top page by entering "**http://192.168.0.254:8080**" into the web browser's address bar.
- When accessing Setup from the top page, an authentication window is displayed (after starting the web browser, first time only). Log in by entering your user name and password and clicking [OK].
- In order to view the camera images on the Camera Portal page of this product, it is necessary to have completed a connection with a compatible camera (Customer-provided). See the camera's manuals for more details.

If the top page is not displayed...

- Confirm that "**http://bbhgw.webpage:8080**" is entered correctly in the address bar (the default port number is 8080). If the address is correct and the top page is still not displayed enter "**http://192.168.0.254:8080**".
- Confirm that the LAN indicator corresponding to the jack connected to this product is on.
- Confirm that this product's power was turned on before the PC's power was.
- Sometimes it is necessary to set up the web browser's proxy server to access the top page (see page 131).

2.1.2 Setup

This page allows you to set up an IPv4 Internet connection using your PC's web browser.
The heading selected on the menu page is displayed on the main page.
The help page describes the operations of each heading.


Panasonic
Network Camera
Management System
BB-HGW700
① Top
② Setup
③ IPv6 Setup
④ Camera Portal
Basic Setup
⑤ ISP Registration
⑥ Connection Mode
⑦ Camera
⑧ Wireless
⑨ DynamicDNS
Advanced Setup
⑩ Address Translation
⑪ Security
⑫ Options
⑬ VPN(PPTP)
⑭ VPN(IPsec)
⑮ Applications
Maintenance
⑯ Password
⑰ Update Firmware
⑱ Save Settings
⑲ Restart
⑳ Factory Default
㉑ PPPoE Connection
㉒ VPN(IPsec) Connection
㉓ Ping
Information
㉔ Status
㉕ Log
㉖ Support
㉗ Help
ISP Registration
Clicking the Register/Edit button allows you to register a new ISP or to modify the configuration of a registered ISP. Clicking Connection Mode on the left Menu allows you to change the connection mode or desired ISP.
Note: The settings are managed in connection with each ISP Name.
Up to 4 ISPs can be registered.
ISP Registration List
No. | ISP Name | Mode | Register/Edit | Status | Delete
1 | ****** | Static | Register/Edit | Enable | Delete
2 | | No Entry | Register/Edit | | Delete
3 | | No Entry | Register/Edit | | Delete
4 | | No Entry | Register/Edit | | Delete
Click here to switch to other ISPs.
When the Status field indicates "Disable", confirm whether the Internet connection mode is correctly selected.
Menu
Main

① Top:	Displays the top page. (see page 11)
② Setup:	Displays the setup page. It is possible to set up all operations from this page. (see this page)
③ IPv6 Setup:	Displays the IPv6 setup page. (see page 16)
④ Camera Portal:	Allows you to view images from the camera registered on this product. (see page 17)

Basic Setup

⑤ ISP Registration:	Basic setup to connect to the Internet. (see page 22)
⑥ Connection Mode:	Sets the connecting ISP. (see page 38)
⑦ Camera:	Performs automatic camera registration setup and manual registration adding and deletion. (see page 40)
⑧ Wireless:	Sets up wireless LAN motion mode and wireless security. (see page 48)
⑨ DynamicDNS	Sets up DynamicDNS. (see page 56)

Advanced Setup

⑩ Address Translation:	Translates both the global address on the WAN side (Internet) and private address on the LAN side, and also performs setup to access this product's network from an Internet terminal. (see page 60)
⑪ Security:	Allows you to set up filtering, and control access to this product at the touch of a button, and automatically saves a log. (see page 66)
⑫ Options:	Sets up access on the LAN side, and also connection to the Internet. (see page 77)
⑬ VPN (PPTP):	By setting a user name and password, this product allows you to create a VPN (Virtual Private Network) using PPTP (Point-to-Point Tunneling Protocol). (see page 88)
⑭ VPN (IPsec)	By setting security policy database, this product allows you to create a VPN using IPsec. (see page 90)
⑮ Applications:	This function allows you to register, execute and delete applications for use with this product. (see page 98)

Maintenance

⑯ Password:	Modifies the user name and password to access the setup page. (see page 101)
⑰ Update Firmware*:	Updates to the latest version of firmware. (see page 102)
⑱ Save Settings:	Saves and loads settings. (see page 104)
⑲ Restart:	Restarts this product. (see page 105)
⑳ Factory Default:	Initializes this product. The settings are returned to the factory default. (see pages 105 and 117)
㉑ PPPoE Connection:	Manually starts or stops the PPPoE connection to the ISP. (see page 106)
㉒ VPN (IPsec) Connection	Manually starts or stops the VPN (IPsec) connection to the ISP. (see page 107)
㉓ Ping:	Checks that each device with an IP address is connected. (see page 108)

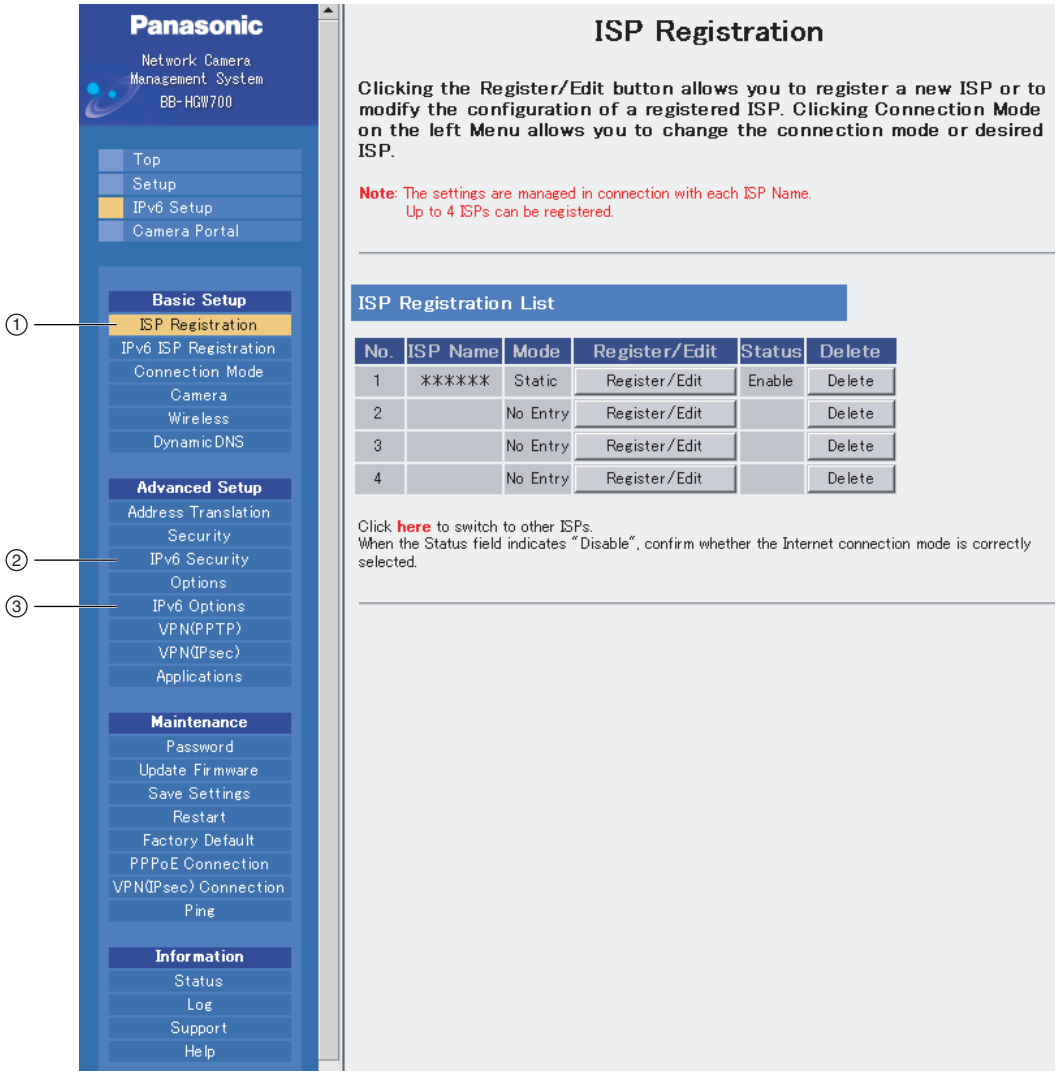
Information

㉔ Status:	Displays information such as connection status. (see page 109)
㉕ Log:	Displays Filtering Log, UPnP Log (general), UPnP Log (CP), Connection Log, DynamicDNS Log, VPN (PPTP) Connection Log, VPN (IPsec) Connection Log, Mail Transmission Log, and VPN (IPv4 IPsec) Connection Log. (see page 112)
㉖ Support:	Product and support information can be found on the Internet. (see page 116)
㉗ Help:	Explains about commands and functions on the setup pages. (see page 116)

* To download the latest version of the firmware from Panasonic's support website, it is necessary to connect to the Internet.

2.1.3 IPv6 Setup

This page allows you to set up an IPv6 Internet connection using your PC's web browser.
The heading selected on the menu page is displayed on the main page.
The Help page describes the operations of each heading.



① IPv6 ISP Registration: IPv6 basic setup to connect to the Internet. (see page 30)

② IPv6 Security: Allows you to set up IPv6 filtering, and control access to this product at the touch of button, and automatically saves a log. (see page 72)

③ IPv6 Options: Sets up access on the LAN side, and various other IPv6 options. (see page 85)

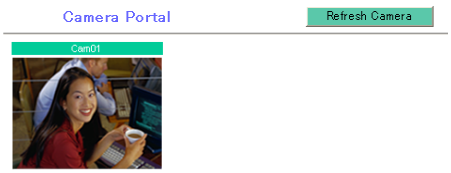
2.1.4 Camera Portal

This product has a built in web server function. Camera Portal allows you to list up to 16 cameras names and their still images.

Viewing Camera Images from the LAN (Home) Side

It is possible to view camera images by accessing the camera portal.

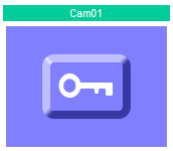
1. Start the web browser.
2. Enter "**http://bbhgw.webpage:port number**" into the web browser's address bar.
   - (e.g. **http://bbhgw.webpage:80**
     The default port number is 80. If the port number is 80, there is no need to enter it.)
   - The camera portal is displayed.
   - By clicking on the still image, a single moving image can be displayed.
   - When Microsoft® Windows XP Service Pack 2 is used, a pop-up blocker may prevent the camera from displaying the image. See page 118 about a pop-up blocker.



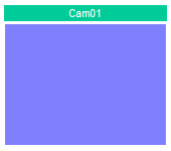
Notes

- If an exclamation mark is displayed, click it and the camera's password window is displayed. Perform the settings on each page. Setting Allow Access from the Internet to Enable, displays the camera images on the Camera Portal over the Internet. Setting Disable only displays the camera images on the Camera Portal when accessing from the LAN side.
  (It is displayed when a factory default camera is connected.)

- If a key mark is displayed, click it and enter that camera's user name and password.
  (If camera authentication has been set up, the key mark will be displayed.)



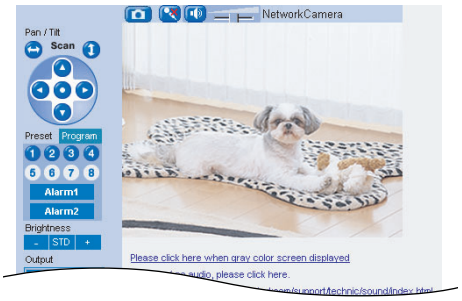
- A blue unmarked window is displayed when the camera is outside operation time. If a blue unmarked window is displayed even when the camera is operating, click [Refresh Camera].
  (The blue unmarked window may be displayed when authentication is being confirmed.)



- If the camera and this product are disconnected while sending or receiving data, a key mark (when camera authentication is set up) or a blue unmarked window is displayed. In this case, after checking that the camera's power supply and connections are correctly inserted, click [Refresh Camera].

3. Click the camera frame you want to access.

- If an authentication window is displayed, enter the camera's user name and password. Then the camera image is displayed.



Notes

- When refreshing the camera portal, click [Refresh Camera] on the Camera Portal page.
- After entering the camera's user name and password and displaying the camera image once, the camera image will be displayed on the camera portal without the key mark. When displaying other pages such as setup, the key mark will return, but by clicking it, the camera image will be displayed without the authentication window.

Privacy and Image Right

When installing and using this camera, it is the customers responsibility to not infringe on privacy or copyright rules and regulations.

* It is generally accepted that "Privacy is the legal right to not have one's private life displayed in public, and the right to have control over one's own personal information. Image right is the right to not have portraits or photographic images of one's self created by a stranger or displayed in public".

When camera images are not displayed on the camera portal...

- Check that the WAN indicator and the LAN indicator corresponding to the jack connected to this product is on.
- Sometimes it is necessary to set up the web browser's proxy server to access the camera portal (see page 131).
- Check that the power supply was turned on in the following order: modem, this product, PC.
- When a camera name, an X mark, a blue unmarked window, or a white page is displayed on the camera portal, click [Refresh Camera].
- When an exclamation mark is displayed on the camera portal, click it. The camera's password window is displayed.

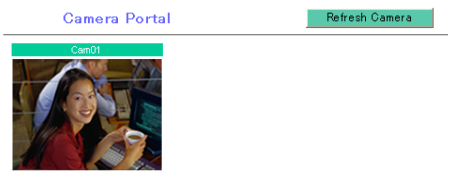
Viewing Camera Images from the WAN (Internet) Side

This function allows you to view camera images by accessing the camera portal from the WAN side.

Note

To view camera images from the Internet, it is necessary to connect this product to your modem and have an Internet subscription. Regarding how to connect to the Internet see Installation/ Troubleshooting and Using the Functions (see page 22).

1. Start the web browser.
2. Enter "**http:// IP address(WAN) or URL : port number**" into the web browser's address bar.
   - (e.g. **http://10.75.68.251:80**
     http://www.example.com:80
     The default port number is 80. If the port number is 80, there is no need to enter it.)



Notes

- It is possible to check the status of the IP address (WAN) on the setup pages. (see page 109)
- When using this product with a service that is not a static IP service, the IP address changes. It is recommended that you use the Viewnetcam.com service. (see page 56)

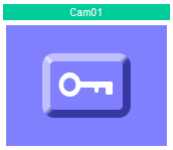
3. Press [Enter].
   - The camera portal is displayed.
   - By clicking on the still image, a single moving image can be displayed.
   - When Microsoft Windows XP Service Pack 2 is used, a pop-up blocker may prevent the camera from displaying the image. See page 118 about a pop-up blocker.

Notes

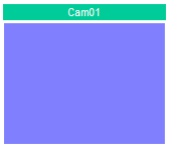
- In order to open an IPv6 camera with an IPv6 address using the Camera Portal, first, register the camera's IPv6 address with an IPv6 compatible DynamicDNS service (e.g. Viewnetcam.com). Then, register the camera manually on this product (To register a domain name to the IPv6 camera settings, see page 44), and set it on the Camera Portal.
- In order to use IPv6 your local network, your ISP must support IPv6. Please contact your local network administrator or ISP if you have any questions.

- If an exclamation mark is displayed, click it and the camera's password window is displayed. Perform the settings on each page. Setting Allow Access from the Internet to Enable, displays the camera images on the Camera Portal over the Internet. Setting Disable only displays the camera images on the Camera Portal when accessing from the LAN side.
(It is displayed when a factory default camera is connected.)

- If a key mark is displayed, click it and enter that camera's user name and password.
(If camera authentication has been set up, the key mark will be displayed.)

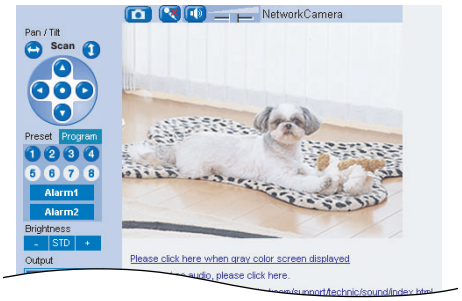


- A blue unmarked window is displayed when the camera is outside operation time. If a blue unmarked window is displayed even when the camera is operating, click [Refresh Camera].
(The blue unmarked window may be displayed when authentication is being confirmed.)
- If the camera and this product are disconnected while sending or receiving data, a key mark (when camera authentication is set up) or a blue unmarked window is displayed. In this case, after checking that the camera's power supply and connections are correctly inserted, click [Refresh Camera].



4. Click the camera frame you want to access.

- If an authentication window is displayed, enter the camera's user name and password. Then the camera image is displayed.



If the camera portal is not displayed...

- Check that "**http:// IP address(WAN) or URL : port number**" was entered correctly into the address bar.
- Sometimes it is necessary to set up the web browser's proxy server to access the website. (see page 131)
- When a camera name, an X mark, or a white page is displayed on the camera portal, click [Refresh Camera].

Notes

- All user information (video images, still images, Internet contents etc.) is the responsibility of the customer. Access to this information should be limited to users or user groups, and third parties should not be allowed to refer to, modify, delete or copy this information.
- When changing the setup of the camera or camera portal, see Using Camera. (see page 40)

Privacy and Image Right

When installing and using this camera, it is the customers responsibility not to infringe on privacy or copyright rules and regulations.

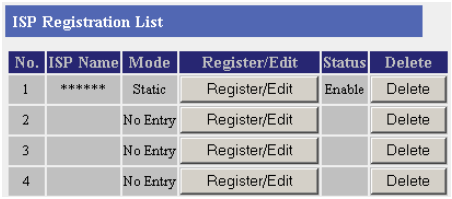
* It is generally accepted that "Privacy is the legal right not to have one's private life displayed in public, and the right to have control over one's own personal information. Image right is the right to not have portraits or photographic images of one's self created by a stranger or displayed in public".

3 Functions

3.1 Using the Functions

3.1.1 Registering ISPs

The ISP registration page allows you to register new ISPs (see page 23) for this product, edit them, and delete them (see page 29). Internet connection methods vary according to the ISP. Select a connection method referring to the ISP's setup information.



Consult with your contracted ISP about which connection type to use, or about your service or contract.

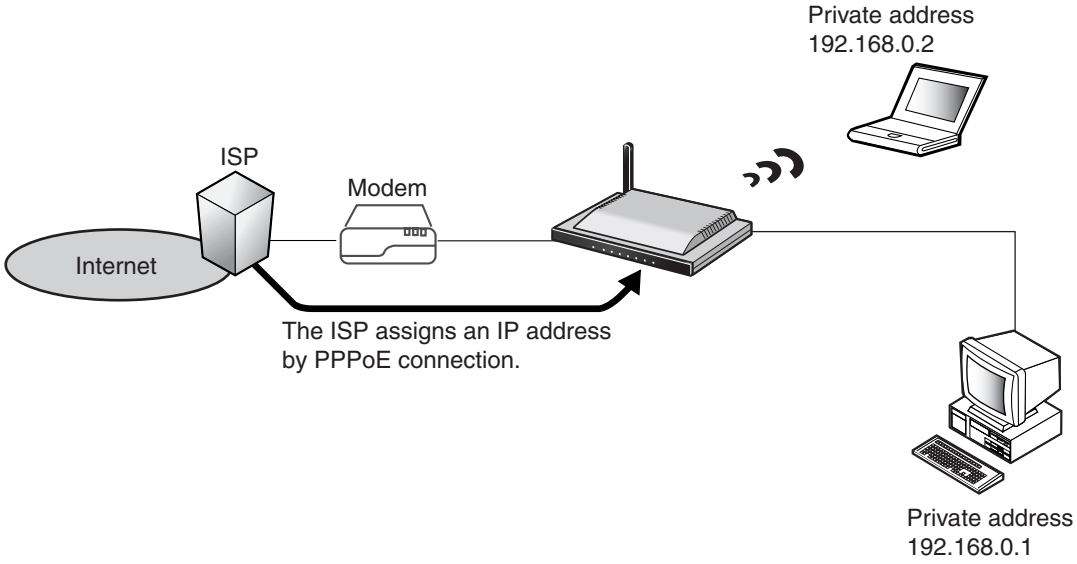
Data Entry Field

Connection Type	Description
PPPoE (see page 23) • ISP Name • User Name/Password • Service Name • Access Concentrator Name • DNS Server 1/DNS Server 2 • Domain Name	It is necessary to enter the following data when using PPPoE connection. Enter the user name and password referring to the ISP's setup information. Enter the service name, access concentrator name DNS server 1, DNS server 2, and/or domain name if specified by the ISP.
DHCP (see page 25) • ISP Name • Device Name • Gateway • DNS Server 1/DNS Server 2 • Domain Name	When the ISP is using a DHCP server, setup entry is not essentially necessary. However, sometimes it is necessary to enter the device name, gateway, DNS server 1, DNS server 2, and/or domain name. Enter them referring to your ISP's setup information.
Static (see page 27) • ISP Name • IP Address • Subnet Mask • Gateway • DNS Server 1/DNS Server 2 • Domain Name	Enter the IP address, subnet mask, gateway, DNS server 1, and DNS server 2 specified by the ISP. Enter the domain name if specified by the ISP.

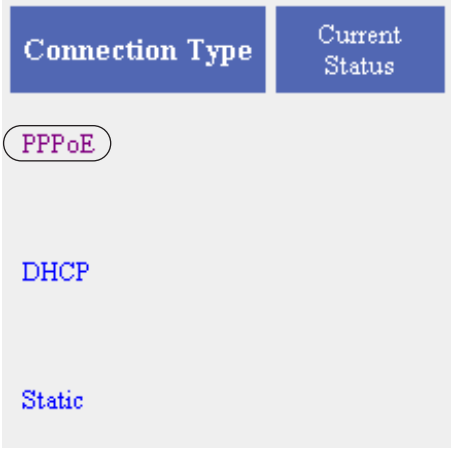
* If it is not necessary to enter information into the data entry field, leave it blank.

PPPoE Connection

Follow the steps below to set up PPPoE connection.

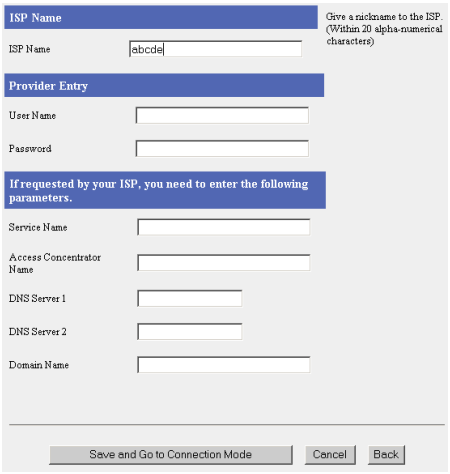


1. Select [ISP Registration].
2. Click [Register/Edit] on the ISP registration list.
3. Select PPPoE.



4. Enter ISP Name.
- Enter no more than 20 characters. In the example right, "abcde" has been entered.

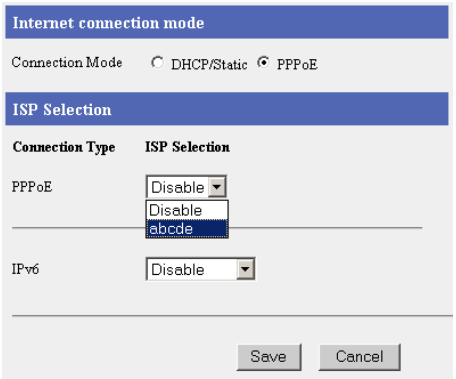
5. Enter User Name and Password, and if specified by the ISP, enter Service Name, Access Concentrator Name, DNS Server 1, 2, and/or Domain Name.
- See the ISP's setup information. To return to the original settings, click [Cancel].



6. When setup is complete, click [Save and Go to Connection Mode].
- The connection mode page is displayed.

7. Select the ISP entered in step 4.

8. When setup is complete, click [Save].
- The entered information is saved.



Note

When saving, do not cut the power supply. If cut, saving might not be completed successfully.

9. When [Restart] is displayed on the setup page, click it.

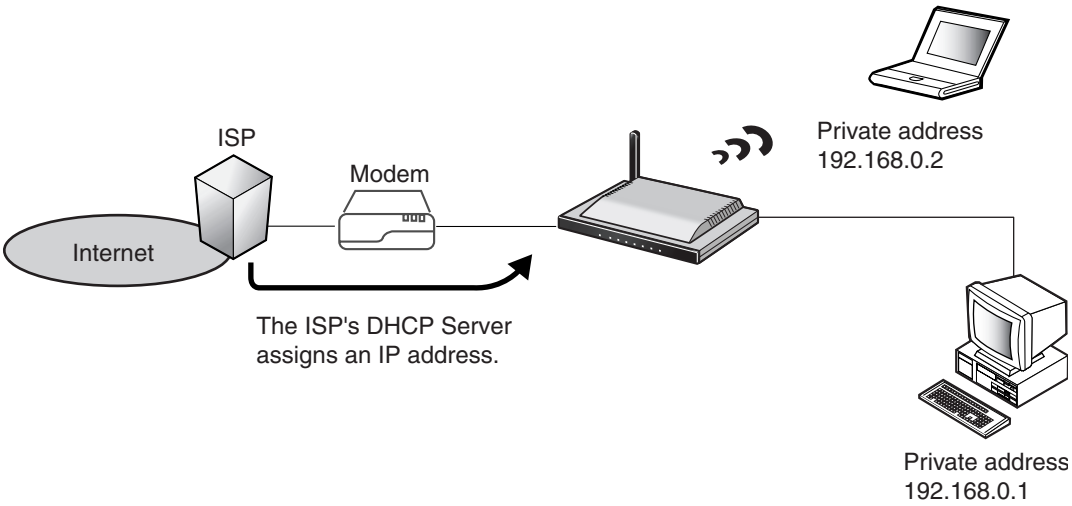
10. Restart the PC.
- Check that the PC is connected to the Internet. (see page 37)

New settings are saved.
It is necessary to restart this product to complete the setting.
If you want to restart later, click the restart button on the restart page.
If you want to restart it immediately, click the restart button below.
Restart

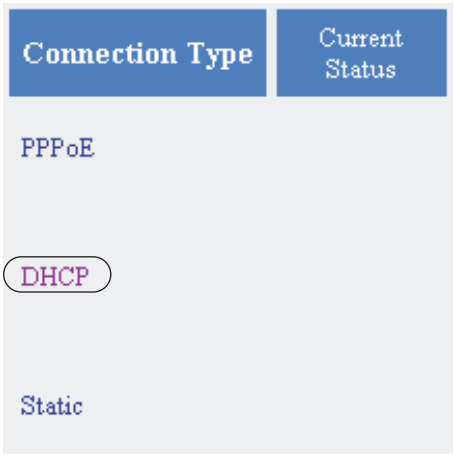
Notes
- When registering or editing, restart all PCs connected to the LAN (home) side.
- When adding more PCs after setup has been completed, connect the new PCs to jacks LAN1 to LAN4 and then restart.
- When instructed by your ISP, change the MTU value. When not instructed, leave it as the default (1492). (see page 80)

DHCP Connection (Internet Connection using a DHCP Server)

Follow the steps below to set up DHCP connection, where an IP address is automatically allocated by the ISP.

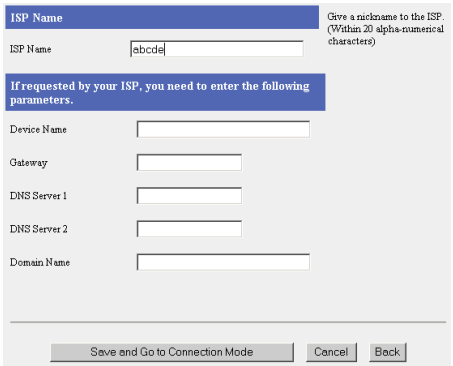


1. Select [ISP Registration].
2. Click [Register/Edit] on the ISP registration list.
3. Select DHCP.



4. Enter ISP Name.
   - Enter no more than 20 characters. In the example right, "abcde" has been entered.
5. If specified by the ISP, enter Device Name*, Gateway, DNS Server 1, 2, and/or Domain Name.
   - See the ISP's setup information. To return to the original settings, click [Cancel].

   * The device name is sometimes said by the ISP to be the ID entered into the PC's Computer Name entry field.

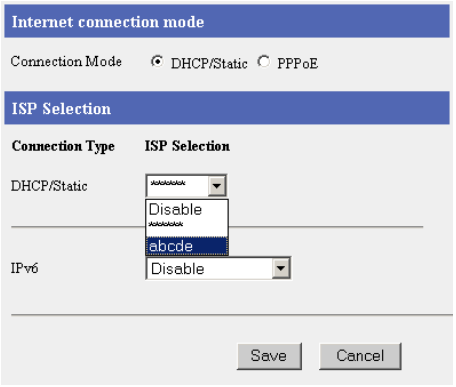


Functions

6. When setup is complete, click [Save and Go to Connection Mode].
- The connection mode page is displayed.

7. Select the ISP entered in step 4.

8. When setup is complete, click [Save].
- The entered information is saved.



Note

When saving, do not cut the power supply. If cut, saving might not be completed successfully.

9. When [Restart] is displayed on the setup page, click it.

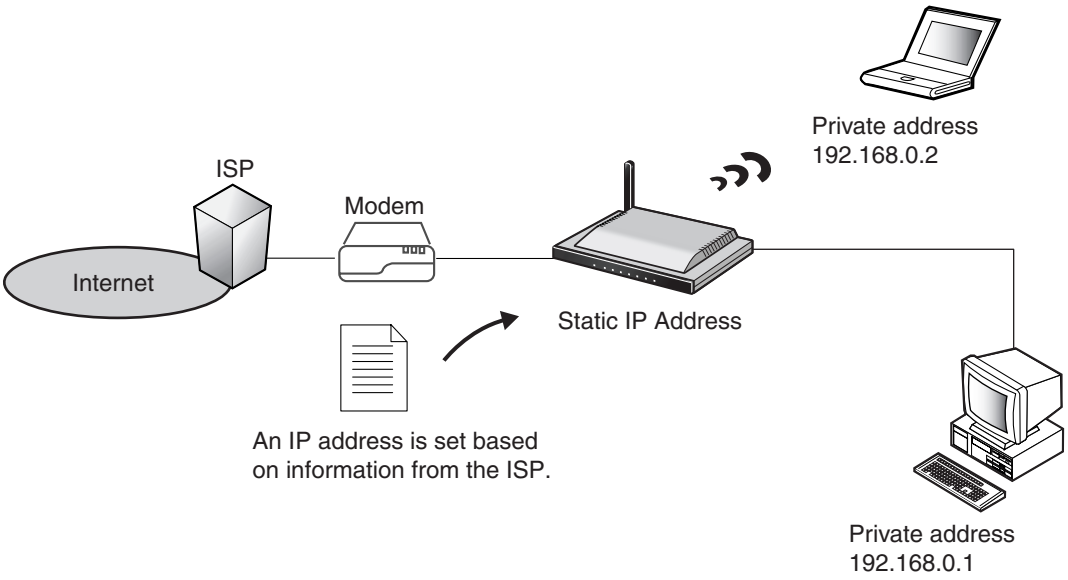
10. Restart the PC.
- Check that the PC is connected to the Internet. (see page 37)

New settings are saved.
It is necessary to restart this product to complete the setting.
If you want to restart later, click the restart button on the restart page.
If you want to restart it immediately, click the restart button below.
Restart

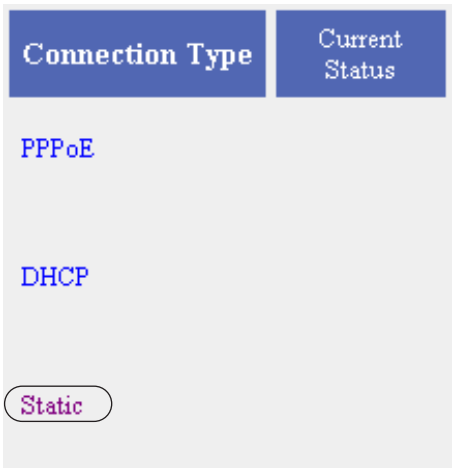
Notes
- When registering or editing, restart all PCs connected to the LAN (home) side.
- When adding more PCs after setup has been completed, connect the new PCs to jacks LAN1 to LAN4 and then restart.

Static Connection (Internet Connection using a Static IP Address)

It may be necessary, if you are instructed by the ISP, to enter the value of the IP address or gateway address into setup information.

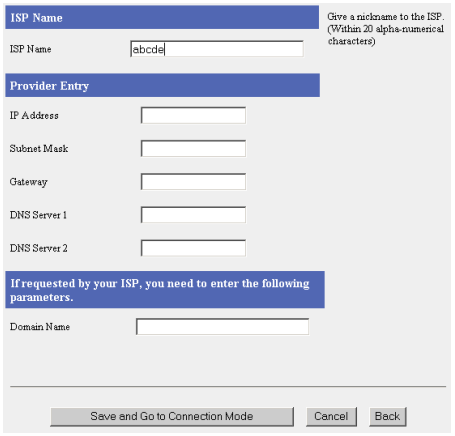


1. Select [ISP Registration].
2. Click [Register/Edit] on the ISP registration list.
3. Select Static.



4. Enter ISP Name.
- Enter no more than 20 characters. In the example right, "abcde" has been entered.

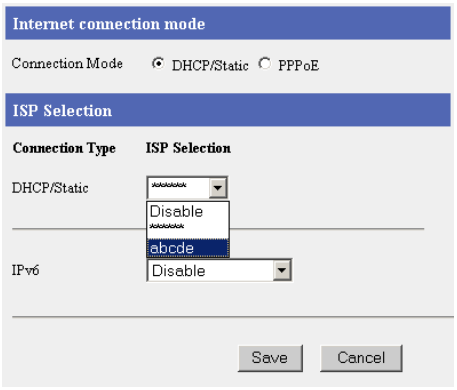
5. Enter the IP Address, Subnet Mask, Gateway and DNS server 1, 2, and if specified by the ISP, enter the Domain Name.
- See the ISP's setup information. To return to the original settings, click [Cancel].



6. When setup is complete, click [Save and Go to Connection Mode].
- The connection mode page is displayed.

7. Select the ISP entered in step 4.

8. When setup is complete, click [Save].
- The entered information is saved.

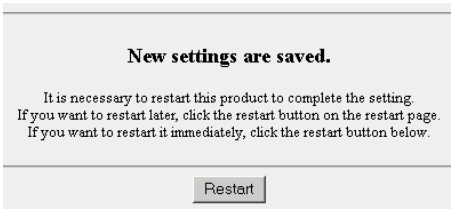


Note

When saving, do not cut the power supply. If cut, saving might not be completed successfully.

9. When [Restart] is displayed on the setup page, click it.

10. Restart the PC.
- Check that the PC is connected to the Internet. (see page 37)

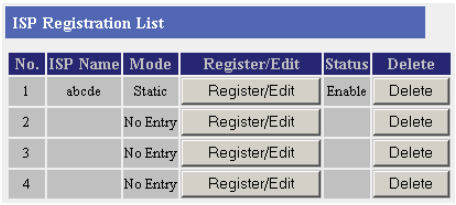

New settings are saved.
It is necessary to restart this product to complete the setting.
If you want to restart later, click the restart button on the restart page.
If you want to restart it immediately, click the restart button below.
Restart

Notes
- When registering or editing, restart all PCs connected to the LAN (home) side.
- When adding more PCs after setup has been completed, connect the new PCs to jacks LAN1 to LAN4 and then restart.

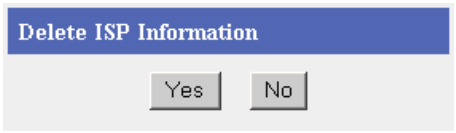
ISP Deletion

Follow the steps below to delete ISPs from the ISP registration list/IPv6 ISP Registration List.

1. Click [Delete] on the row of the ISP you want to delete.
- The ISP deletion confirmation window is displayed.


ISP Registration List
No. ISP Name Mode Register/Edit Status Delete
1 abcde Static Register/Edit Enable Delete
2 No Entry Register/Edit Delete
3 No Entry Register/Edit Delete
4 No Entry Register/Edit Delete

2. Click [Yes].
- To cancel the deletion click [No].

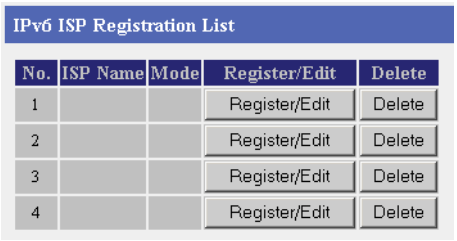


3. When [Restart] is displayed on the setup page, click it.

New settings are saved.
It is necessary to restart this product to complete the setting.
If you want to restart later, click the restart button on the restart page.
If you want to restart it immediately, click the restart button below.
Restart

3.1.2 Registering IPv6 ISPs

This heading is only displayed when IPv6 Setup is selected on the menu. On the IPv6 ISP Registration List it is possible to register, edit and delete IPv6 ISPs to connect to this product. Methods of connection to the IPv6 network are different depending on the ISP. Select a connection type referring to information from your ISP.



Consult with your contracted ISP about which IPv6 connection type to use, or about your service or contract.

Data Entry Field

Connection Type	Description
Tunneling (see page 31) • ISP Name • Destination IP Address • Prefix(LAN) • IPv6 DNS Server 1/ IPv6 DNS Server 2 • IPv6 Address(WAN)	Enter the Destination IP Address and Prefix(LAN) specified by the ISP. Enter the IPv6 DNS Server 1, IPv6 DNS Server 2, and/or IPv6 Address(WAN) if specified by the ISP.
6to4 (see page 33) • ISP Name • Destination IP Address	6to4 is a connection mode being used experimentally to verify the mutual connectivity of IPv4 and IPv6. Set the destination IP address seeing the website describing 6to4 addressing.
Static v6 (see page 35) • ISP Name • IPv6 address(WAN) • Prefix(LAN) • IPv6 Default Gateway • IPv6 DNS Server 1/ IPv6 DNS Server 2 • Domain Name	Enter the IPv6 Address(WAN), Prefix(LAN), IPv6 Default Gateway, IPv6 DNS Server 1, and IPv6 DNS Server2 specified by the ISP. Enter Domain Name if specified by the ISP.

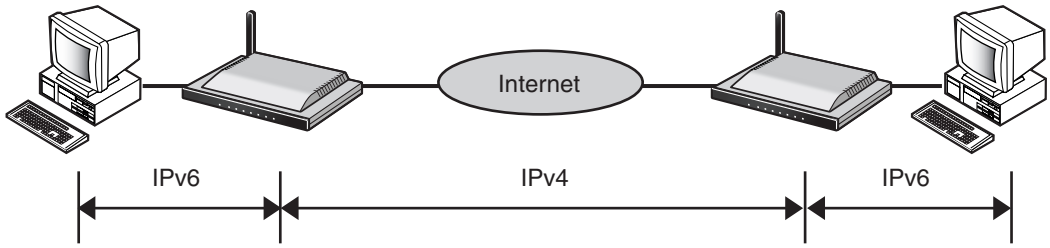
* If it is not necessary to enter information into the data entry field, leave it blank.

What is IPv6?

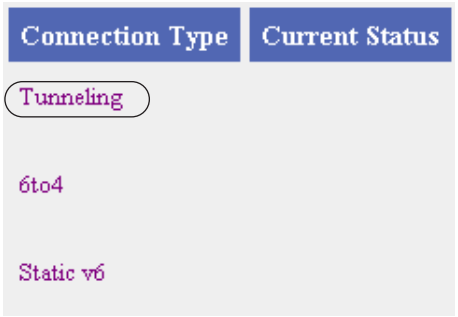
- IPv6 is short for "Internet Protocol Version 6".
- IPv6 was created to address the additional IP addresses that will be needed as the Internet continues to expand.
- IPv6 is expected to gradually replace IPv4, with the 2 coexisting for a number of years during a transition period.
- Though most ISPs (Internet Service Providers) do not yet support IPv6, many local networks already use it. When your ISP supports IPv6, your Panasonic Network Camera Management System will be ready!
- For more information you wish to visit **http://www.ipv6.org/**.

Tunneling Connection

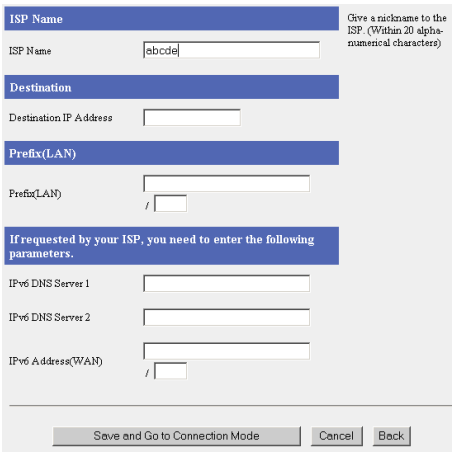
It is possible to encapsulate IPv6 packets with IPv4 packets and perform IPv6 communication on a IPv4 network. Take the following steps to set up tunneling connection.



1. Select [IPv6 ISP Registration].
2. Click [Register/Edit] on the IPv6 ISP registration list.
3. Select Tunneling.

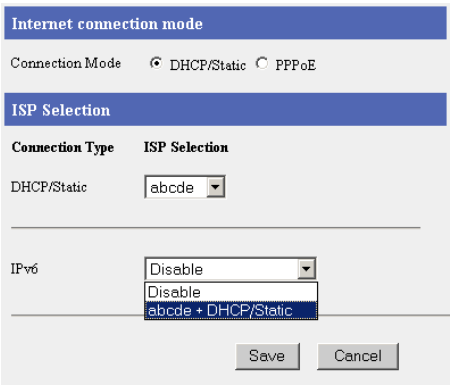


4. Enter ISP Name.
   - Enter no more than 20 characters. In the example right, "abcde" has been entered.
5. Enter the Destination IP Address and Prefix(LAN), and if specified by the ISP, enter the IPv6 DNS Server 1, IPv6 DNS Server 2, and/or IPv6 Address(WAN).
   - See the ISP's setup information. To return to the original settings, click [Cancel].



6. When setup is complete, click [Save and Go to Connection Mode].
   - The connection mode page is displayed.

7. Select the ISP entered in step 4.



8. When setup is complete, click [Save].

- The entered information is saved.

Note

When saving do not cut the power supply. If cut, saving might not be completed successfully.

9. When [Restart] is displayed on the setup page, click it.

New settings are saved.
It is necessary to restart this product to complete the setting.
If you want to restart later, click the restart button on the restart page.
If you want to restart it immediately, click the restart button below.
Restart

10. Restart the PC.

- Check that the PC is connected to the Internet. (see page 37)

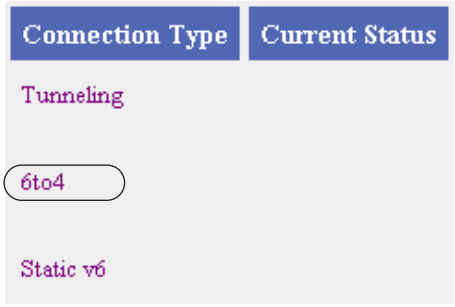
Notes

- When registering or editing, restart all PCs connected to the LAN (home) side.
- When adding more PCs after setup has been completed, connect the new PCs to jacks LAN1 to LAN4 and then restart.

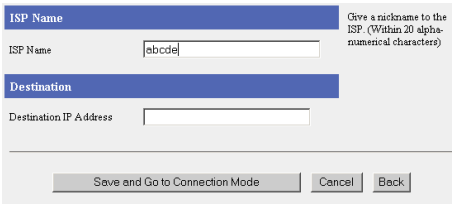
6to4 Connection

6to4 is a type of tunnel connection which can be used experimentally. 6to4 encapsulates IPv6 packets with IPv4 packets, and connects to the IPv6 network through the 6to4 relay router. It is not necessary to subscribe to an ISP for this type of connection. Take the following steps to set up 6to4 connection.

1. Select [IPv6 ISP Registration].
2. Click [Register/Edit] on the IPv6 ISP registration list.
3. Select 6to4.



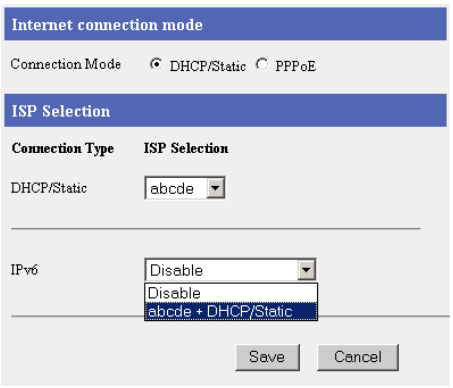
4. Enter ISP Name.
   - Enter no more than 20 characters. In the example right, "abcde" has been entered.
5. Set the destination router's IPv4 Address.
   - To return to the original settings, click [Cancel].



Note

Set a public 6to4 relay router IP address for the destination IP address. The 6to4 relay router is made public and can search the Internet.

6. When setup is complete, click [Save and Go to Connection Mode].
   - The connection mode page is displayed.
7. Select the ISP entered in step 4.
8. When setup is complete, click [Save].
   - The entered information is saved.



Notes

- When saving, do not cut the power supply. If cut, saving might not be completed successfully.
- You must set an IPv4 ISP.
- The WAN side IPv6 global address may change when the WAN side IPv4 global address is changed, because 6to4 connection is dependent upon the IPv4 global address.

9. When [Restart] is displayed on the setup page, click it.

New settings are saved.
It is necessary to restart this product to complete the setting.
If you want to restart later, click the restart button on the restart page.
If you want to restart it immediately, click the restart button below.
Restart

10. Restart the PC.

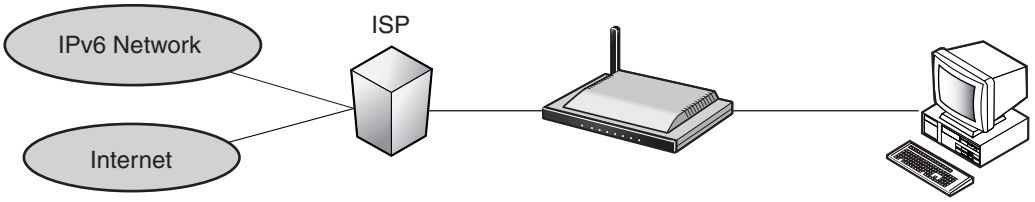
- Check that the PC is connected to the Internet. (see page 37)

Notes

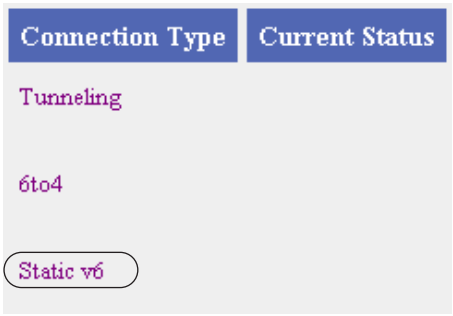
- When registering or editing, restart all PCs connected to the LAN (home) side.
- When adding more PCs after setup has been completed, connect the new PCs to jacks LAN1 to LAN4 and then restart.

Static v6 Connection

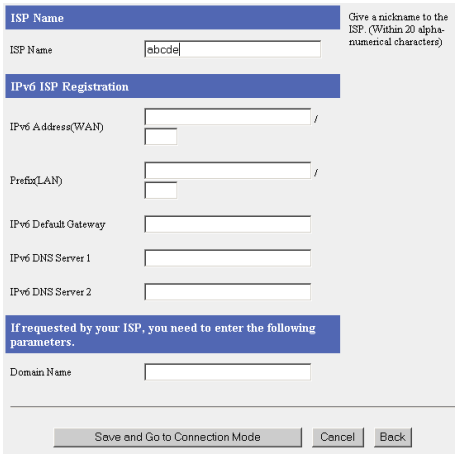
This function allows you to communicate directly using IPv6. To set up static v6 connection, take the following steps.



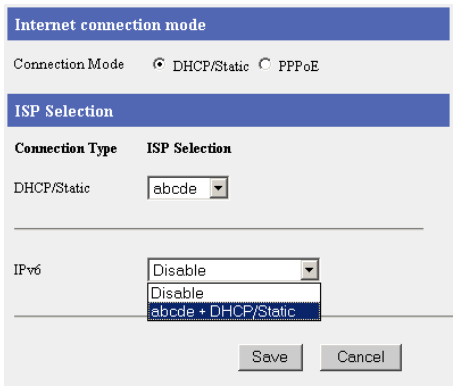
1. Select [IPv6 ISP Registration].
2. Click [Register/Edit] on the IPv6 ISP registration list.
3. Select Static v6.



4. Enter ISP Name.
   - Enter no more than 20 characters. In the example right, "abcde" has been entered.
5. Enter the IPv6 Address(WAN), Prefix(LAN), IPv6 Default Gateway, IPv6 DNS Server 1, and IPv6 DNS Server2, and if specified by the ISP, enter the Domain Name.
   - See the ISP's setup information. To return to the original settings, click [Cancel].



6. When setup is complete, click [Save and Go to Connection Mode].
   - The connection mode page is displayed.
7. Select the ISP entered in step 4.

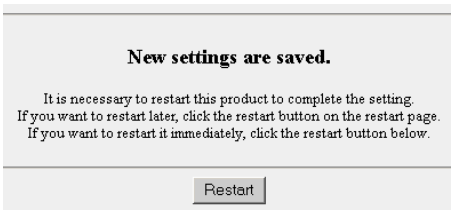


8. When setup is complete, click [Save].
- The entered information is saved.

Note

When saving, do not cut the power supply. If cut, saving might not be completed successfully.

9. When [Restart] is displayed on the setup page, click it.


New settings are saved.
It is necessary to restart this product to complete the setting.
If you want to restart later, click the restart button on the restart page.
If you want to restart it immediately, click the restart button below.
Restart

10. Restart the PC.
- Check that the PC is connected to the Internet. (see page 37)

Notes
- When registering or editing, restart all PCs connected to the LAN (home) side.
- When adding more PCs after setup has been completed, connect the new PCs to jacks LAN1 to LAN4 and then restart.
- For deleting IPv6 ISPs, see page 29.

3.1.3 Confirming Connection to the Internet

Confirming Connection

After the setup for Internet connection is complete, try to access a website. If the website is displayed, you have successfully connected to the Internet.

1. Start the web browser.
2. Enter a website address into the web browser's address bar (e.g. **http://www.panasonic.com**), and press [Enter].
   - The website is displayed.

When a website is not displayed...

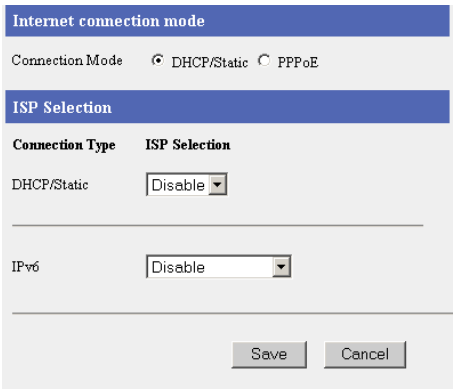
- Check that the website address was entered correctly in the web browser's address bar.
- Check that the WAN and LAN indicators corresponding to the WAN and LAN jacks connected to this product are on.
- Check that the power supply was turned on in the following order: modem, this product, PC.
- Sometimes it is necessary to set up the web browser's proxy server to access a website (see page 131).

3.1.4 Managing the Connection Mode

The connection mode page allows you to switch between registered ISPs. On the connection mode page, connecting ISPs which have been registered, can be selected from the LAN (Home) side to the WAN (Internet) side.
The two types of connection mode for ISPs connecting to the WAN (Internet) side are [DHCP/Static] and [PPPoE].

Setting up the DHCP/Static Connection Mode to the WAN (Internet) Side

1. Click Connection Mode on the menu page.
   - The connection mode page is displayed.
2. Confirm that DHCP/Static is selected as the connection mode.
   - It is checked as factory default.
3. Select the ISP on the ISP selection dropdown list.



4. Click [Save].
   - When setup is complete, the restart window is displayed.
5. Click [Restart].

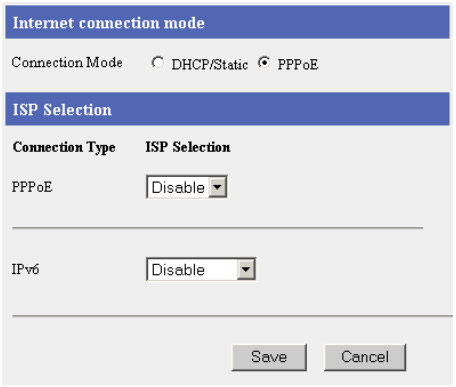
New settings are saved.
It is necessary to restart this product to complete the setting.
If you want to restart later, click the restart button on the restart page.
If you want to restart it immediately, click the restart button below.
Restart

Data Entry Field

ISP Selection	Select only one ISP to use. It is possible to select an IPv6 ISP if one is registered.

Setting up the PPPoE Connection Mode to the WAN (Internet) Side

1. Click Connection Mode on the menu page.
   - The connection mode page is displayed.
2. Select PPPoE as the connection mode.
   - ISP Selection is modified.
3. Select the ISP on the ISP selection dropdown list.



4. Click [Save].
   - When setup is complete, the restart window is displayed.
5. Click [Restart].

New settings are saved.
It is necessary to restart this product to complete the setting.
If you want to restart later, click the restart button on the restart page.
If you want to restart it immediately, click the restart button below.
Restart

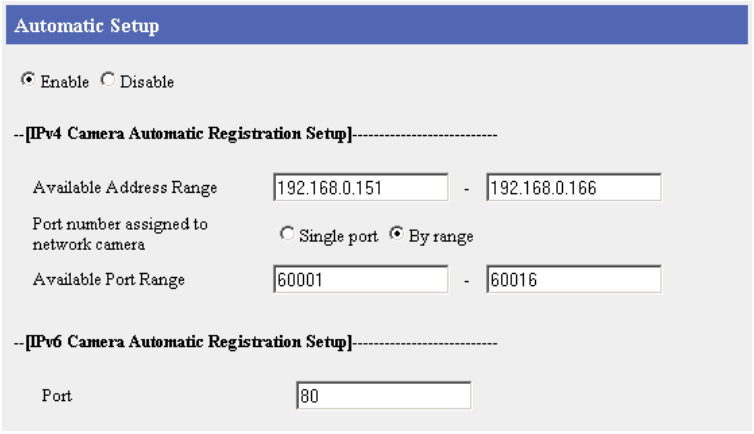
Data Entry Field

ISP Selection	Select only one ISP to use. It is possible to select an IPv6 ISP if one is registered.

3.1.5 Using Camera

The camera page allows you to set up cameras connected to this product.
Usually it is not necessary to set up a camera because the automatic registration function of Panasonic's Network Cameras sets up the camera name, port number, and IP address automatically. When changing a camera name, follow the steps on page 43 - changing the setup of automatically registered cameras. Also, when manually setting up a camera network, register cameras by following the steps in additional camera registration.

Automatic Setup



Data Entry Field

Automatic Setup	Select Enable or Disable.
IPv4 Camera Available Address Range	Specify one sequenced address range to be allocated to the camera. • Be careful that it does not overlap the address allocated by a server, such as a DHCP/PPTP server. • The default is 192.168.0.151 - 192.168.0.166.
Port Number assigned to network camera	Select Single port or By range. • If By range is selected, the value of the Available Port Range is automatically allocated. • Single port can be used in the following situations: 1 When connecting the WAN side to an internal company network, without using address translation. 2 When using only the LAN without connecting to the WAN side.
Available Port Range	Specify the camera port number. • When selecting By range above, it is only possible to specify one sequenced port number range. It is necessary to have the same number of port numbers as available address ranges specified above, so specify the port number range that you will use. • When selecting Single port above, specify one static port number. • The default is 60001-60016.

IPv6 Camera Port	Specify the port number for the IPv6 camera. • The specified port will be provided automatically to IPv6 cameras. • The default is 80.

3.1.6 Registering a Camera Automatically

After connecting this product to a Panasonic Network Camera (Customer-provided), turning the camera on, and returning the settings to factory default, the camera's network setup (IP address and subnet mask etc.) and wireless security setup are performed automatically. After the camera is turned on, this product and the camera exchange information and automatically set up the network. Then, the camera image is registered on the Camera Portal.

Setup Headings

This Product	Port Forwarding Camera Registration Screen Assignment
Camera	Port Number (IPv4) IP Address (IPv4) Port Number (IPv6) DNS Server Address (IPv4/IPv6) Subnet Mask Default Gateway (IPv4) SSID (wireless LAN type only) Encryption Key (wireless LAN type only)

Compatible cameras (Customer-provided) : (as of Mar. 2005)

Indoor type
KX-HCM8
KX-HCM10
KX-HCM250
KX-HCM280
BB-HCM311A
BL-C10A
BL-C30A
BB-HCM381A

Outdoor type
KX-HCM230
KX-HCM270
BB-HCM331A
BB-HCM371A

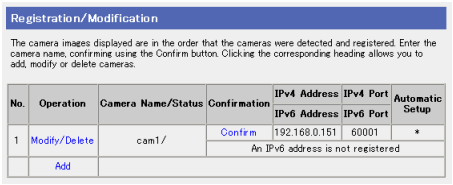
Connecting the Camera without Using Automatic Setup

- When registering all cameras manually, see Additional Camera Registration. (see page 44)

Changing the Setup of Automatically Registered Cameras

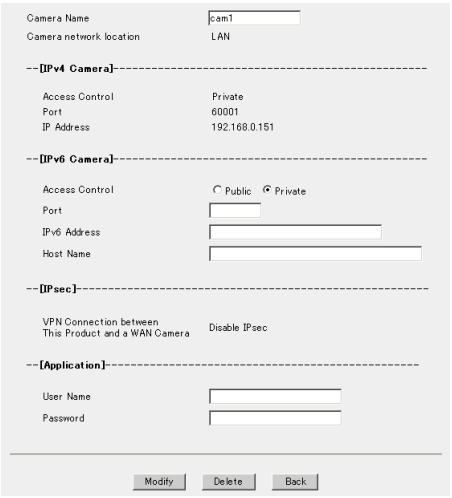
1. Click [Camera] on the setup page.

2. Click Modify/Delete under the Operation heading.



3. Set the required fields and click [Modify].

- To delete a registered camera, click [Delete].



4. When setup is complete, click [Save].

- The entered information is saved.

5. When [Restart] is displayed on the setup page, click it.

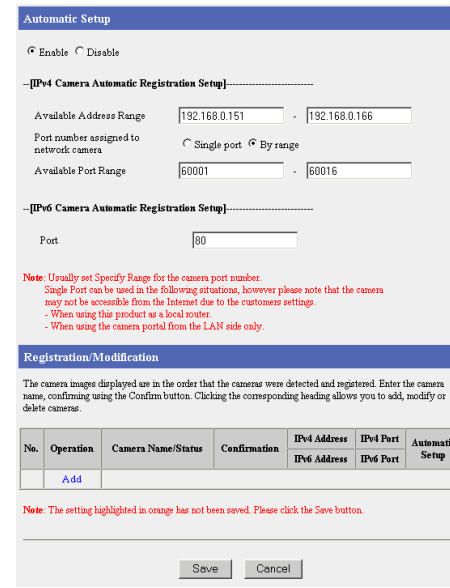
Notes

- With cameras that have the option of enabling images to be accessed from the Internet, follow the setup guidelines specified in the camera's manuals.
- The port number and IP address of automatically registered cameras cannot be modified.
- If you click Confirm, the camera image will appear.
- It may not be possible to open an automatically registered IPv6 camera from the WAN side using the Camera Portal, when using Internet Explorer 6.0 or later. It should be possible to open it using a browser where you can specify an IPv6 address directly into the URL (e.g. Mozilla 1.7.1 or later). However, using a browser other than Internet Explorer 6.0 or later is not under warranty. See page 19 when making camera images accessible from the Internet.

Additional Camera Registration (Registering Additional Cameras Manually)

Follow the steps below to register additional cameras.

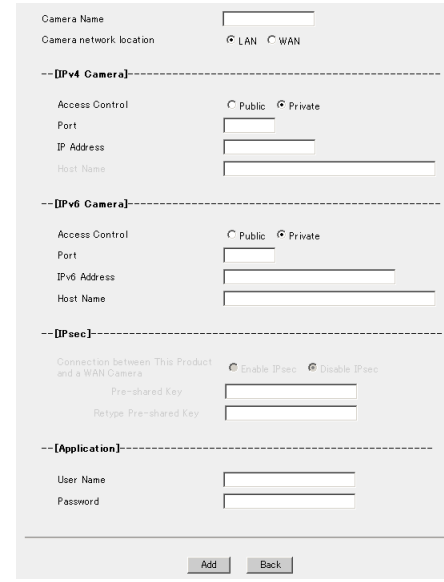
1. Click Add under the Operation heading.


Automatic Setup
Enable
Disable
--[IPv4 Camera Automatic Registration Setup]----------
Available Address Range
192.168.0.151
192.168.0.166
Port number assigned to network camera
Single port
By range
Available Port Range
60001
60016
--[IPv6 Camera Automatic Registration Setup]----------
Port
80
Note: Usually set Specify Range for the camera port number.
Single Port can be used in the following situations, however please note that the camera may not be accessible from the Internet due to the customers settings.
- When using this product as a local router.
- When using the camera portal from the LAN side only.
Registration/Modification
The camera images displayed are in the order that the cameras were detected and registered. Enter the camera name, confirming using the Confirm button. Clicking the corresponding heading allows you to add, modify or delete cameras.
No.
Operation
Camera Name/Status
Confirmation
IPv4 Address
IPv6 Address
IPv4 Port
IPv6 Port
Automatic Setup
Add
Note: The setting highlighted in orange has not been saved. Please click the Save button.
Save
Cancel

2. Enter or Select Camera Name, Camera network location, Access Control, Port, IP Address, Host Name, IPv6 Address, Host Name, and Pre-shared Key if you are using IPsec, and click [Add].

3. When setup is complete, click [Save].

- The entered information is saved.



4. When [Restart] is displayed on the setup page, click it.

5. Follow the instructions on page 47 to add the new camera to the camera portal.

Notes

- When registering an additional camera, modify the settings on the camera side too. For details, see the camera's manuals.
- When registering an additional camera, it is necessary to set port forwarding and/or packet filtering. Set them manually, referring to pages 61, 69, and 74. Also, when using this product under a UPnP™ router, even if the settings for top level routing and address translation are set to Disable, it is necessary to set routing for the other connecting area routers.
- When registering an additional camera, it is necessary to set screen assignment. Set it manually, referring to page 47.
- Neither the DHCP server's Available Address Range specified in LAN IP Address DHCP Server in Options, or the Available Address Range specified in PPTP Server Settings found on the Basic Page of VPN should be set as the IP address range used in the Camera's Automatic Setup.
- It is possible to set the selected camera portal frame to enable it to be accessed from the WAN side, but when registering an additional camera manually, further settings such as filtering (see page 69) or address translation (see page 61) must be performed on this product. When a camera is automatically registered, filtering settings and address translation are performed automatically.
- When manually registering a WAN side camera, it is not possible to view the camera images by clicking Confirm when the camera is Temporarily Saved. Click Confirm after restarting to view the camera images.
- When setting IPsec, enable IPsec on the VPN(IPsec) page.
- When camera images cannot be viewed by clicking Confirm after adding an IPv6 camera, it should be possible to view them using a browser where you can specify an IPv6 address directly into the URL (e.g. Mozilla 1.7.1 or later). However, using a browser other than Internet Explorer 6.0 or later is not under warranty.

Data Entry Field

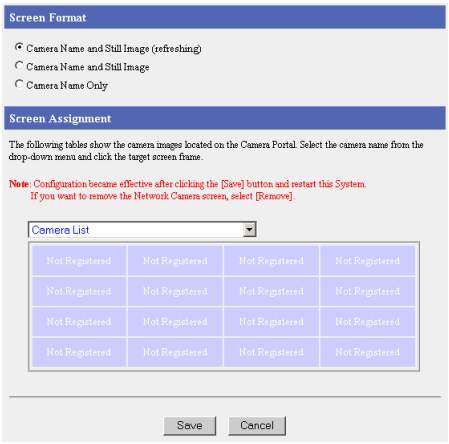
Camera Name	The camera name should be no more than 16 characters.
Camera network location	Check either the LAN side or the WAN side according to the camera's position.
IPv4 Camera Access Control	Set up the connection so that it is either public or private.
Port	Enter the camera's port number.
IP Address	Enter the camera's IP address.
Host Name	When the WAN side is selected for the camera network location, the host name can be specified.
IPv6 Camera Access Control	Set up the connection of the IPv6 camera so that it is either public or private.
Port	Enter the IPv6 camera's port number.
IPv6 Address	Enter the camera's IPv6 address.
Host Name	Enter the host name for the IPv6 camera. The host name can be specified whether the IPv6 camera is on the WAN side or LAN side.

IPsec **Connection between This Product and a WAN camera**	Select Enable IPsec or Disable IPsec.
Pre-shared Key	When Enable IPsec is selected, enter the Pre-shared key.
Retype Pre-shared Key	Retype the same Pre-shared key as above.
Application **User Name**	Enter the user name used for the application function.
Password	Enter the password used for the application function.

Screen Assignment

This function allows you to set the format of the camera portal page and set the screen assignment.

1. Click [Screen Assignment].
2. Select from Camera Name and Still Image (refreshing), Camera Name and Still Image, and Camera Name Only in Screen Format.
3. Select a camera name from the Camera List dropdown list, and click on the camera frame where you want to display it on the Screen Assignment.
   - The selected camera frame is displayed in orange. When removing a camera from the Camera Portal, select Remove the camera from the Camera Portal from the Camera List dropdown list, and click on the camera frame you want to remove on the Screen Assignment.
   - To cancel the current selection, click [Cancel].
4. When setup is complete, click [Save].
   - To return to the original settings, click [Cancel].
5. When [Restart] is displayed on the setup page, click it.
   - The registered camera frame is displayed in green.

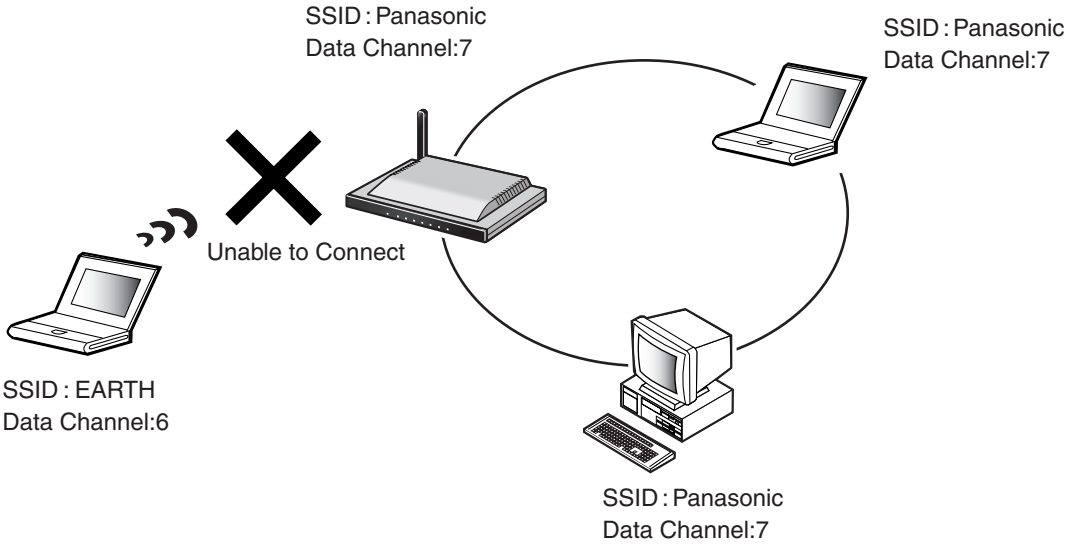

Screen Format
Camera Name and Still Image (refreshing)
Camera Name and Still Image
Camera Name Only
Screen Assignment
The following tables show the camera images located on the Camera Portal. Select the camera name from the drop-down menu and click the target screen frame.
Note: Configuration became effective after clicking the [Save] button and restart this System.
If you want to remove the Network Camera screen, select [Remove].
Camera List
Not Registered
Save
Cancel

Data Entry Field

Screen Format	Select from Camera Name and Still Image (refreshing), Camera Name and Still Image, and Camera Name Only for the screen format.
Screen Assignment	This page allows you to re-position the camera images on the camera portal and register optional cameras. A maximum of 16 camera images can be displayed on the camera portal.

3.1.7 Using Wireless

The wireless setup page allows you to perform settings to connect to wireless LAN and also perform security settings. The wireless LAN uses radio waves in the same way as a TV or transceiver does, selects a data channel, and sends/receives data.
The three data sending modes, "802.11b", "802.11b/g", and "802.11g only", each have differing bands and speeds. The default is all "802.11b/g". Also, it is possible to connect 2 or more wireless devices, by naming (SSID) a network and using the same SSID and data channels for all of them. Set the same SSID and data channel* for all devices on the wireless LAN network.

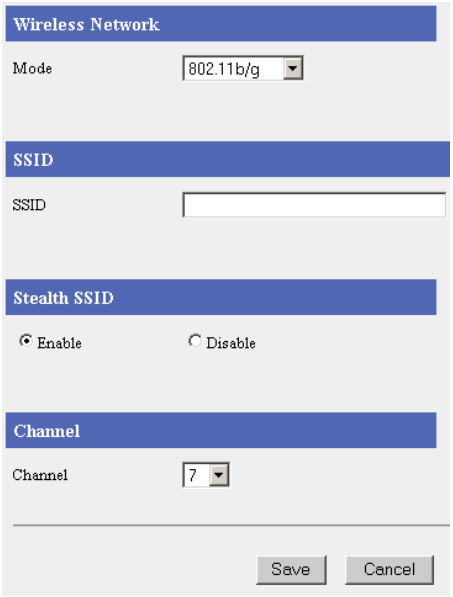


* It is possible for wireless devices connected to this product with the same SSID to send/receive data by searching the data channel automatically.

Note

The default is set as the device-specific SSID and the 13 character 128 bit encryption key. The default SSID and the 13 character 128 bit encryption key are displayed on the rear of this product.

1. Click [Wireless] on the setup page.
2. Enter the SSID into the data entry field, and select a Channel.
   - See page 50 for information about the Stealth SSID.
   - To return to the original settings, click [Cancel].
   - Enter the same SSID into wireless devices connected to this product.
   - The default SSID is displayed on the rear of this product.
   - Regarding each of the data entry fields, see page 50.
3. When setup is complete, click [Save].
   - The entered information is saved.



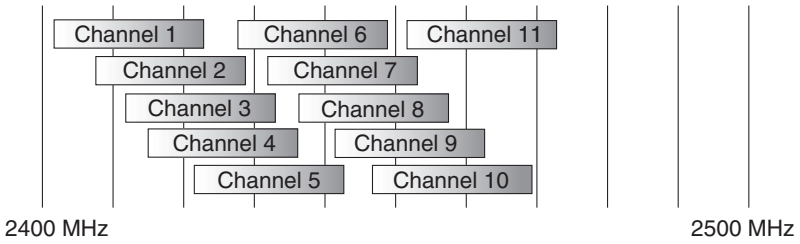
4. When [Restart] is displayed on the setup page, click it.

Notes

- Setting the stealth SSID function to Disable weakens the security.
- Some data channels may be limited by the wireless LAN card used on the wireless terminal side. Check the range of data channels available on the wireless LAN card, and set the data channels on this product accordingly.
- When modifying the SSID of this product after a wireless camera etc. has been registered automatically, it is necessary to match the wireless camera's settings.

Data Entry Field

Wireless Network Mode	Select a wireless network mode from Disable, "802.11b", "802.11b/g" or "802.11g only". • Select Disable when you do not want to send/receive wireless data. • "802.11b" sends/receives data on a 2.4 GHz band. Compatible products are abundant and low priced. Not only is it easy to use, but it is also already widespread so it is useful when you want to use your other wireless devices. • "802.11b/g" sends/receives data on a 2.4 GHz band. It combines the features of "802.11b" and "802.11g", and is compatible with both wireless LAN specifications. It is also easy to introduce into existing wireless environments. • "802.11g only" can only send/receive data to and from the 802.11g. If this product's data sending/receiving mode is set to "802.11g only", it does not support "802.11b/g" integration mode, but the original 802.11g's capabilities are realized. It is faster and reaches further than "802.11b/g", so is good to use when sending/receiving data between floors. • When using "802.11g only", if other 2.4.GHz band wireless devices (including the "802.11b" wireless device) exist, the data speed is reduced.
SSID	A name is given to the network on a wireless LAN. This name is called SSID. The SSID can be set on each device connected to the wireless LAN, and data can only be sent/received to and from devices with the same SSID. Enter the SSID following the guidelines below. (The device-specific SSID is already entered in the default settings. It is displayed on the rear of this product.) • It is case-sensitive. (e.g. 'ABC' and 'abc' are recognized as 2 different names.) • Enter no more than 32 characters.
Stealth SSID	For the wireless LAN device to detect the network, there is a function whereby the SSID, which is a network identifier, is sent out to surrounding devices at regular time intervals. If Disable is selected, the wireless LAN device can detect the network easily. However, unauthorized users can also find the network and try to connect to it, so there a possible security weakness. By selecting Enable on the stealth SSID function, it is possible to use this product to make the network hard to detect for unauthorized users. When Enable is set, connection through the ANY key can be denied. The default is set to Enable.

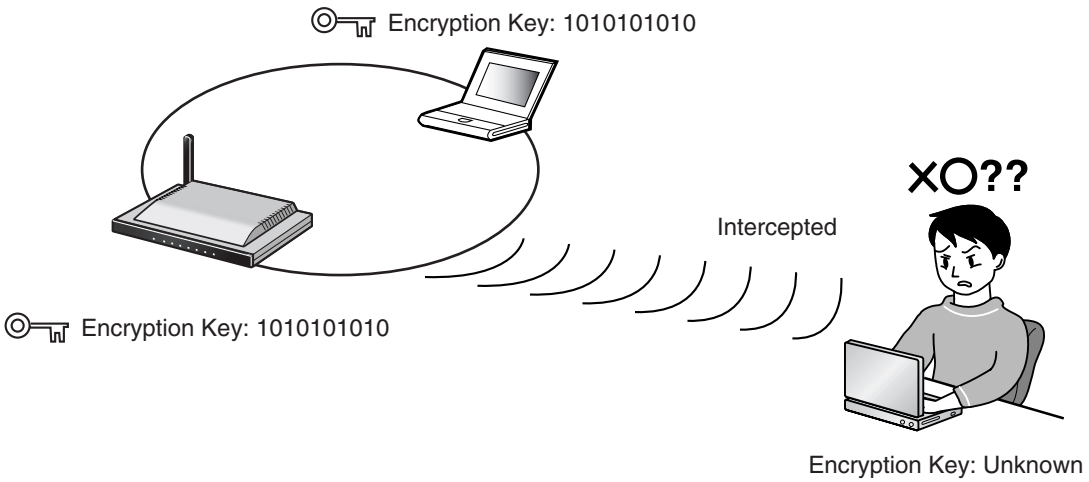
Channel	Sets the channel to receive/send data within the network. Select a channel between 1 and 11. (The default for 802.11b/g is 7.) When there are multiple wireless LANs, and the channel numbers overlap in the figure below (for example, Channel 1 and Channel 4), data speed may be reduced. In that case select a different data channel. 802.11b/802.11g 

Notes

- It is necessary to set the same SSID for the wireless device side and this product.
- If necessary, set Encryption and MAC Address Filtering. To encrypt the sending/receiving data, click Encryption on the Wireless Setup page. (see below) To stop unregistered wireless devices from connecting to this product, click MAC Address Filtering. (see page 55)

Encryption

This function allows you to encrypt sending/receiving data within the wireless LAN. By encrypting the data, even if the data was intercepted by an unauthorized user, it would be illegible. Encryption is performed using the same encryption key for all the registered devices on the wireless LAN.
Always set encryption. If you send unencrypted data, there is a chance that it might be read by a third party or your PC may be invaded etc.
The type of authentication in encryption is not only Shared Key, but also Open System. Authentication conversion is done automatically by this product to match the device.



Notes

- The default is set as the device-specific SSID and the 13 character 128 bit encryption key. The default SSID and the 13 character 128 bit encryption key are displayed on the rear of this product.
- There are 6 types of WEP format: 10 Hexadecimal characters 64 bit, 26 hexadecimal characters 128 bit, 32 hexadecimal characters 152 bit, 5 alpha-numeral characters 64 bit, 13 alpha-numeral characters 128 bit, and 16 alpha-numeral characters 152 bit.
- Cameras are not compatible with WPA, so select WEP when connecting a camera.
- When modifying the encryption of this product after a camera etc. has been registered automatically, it is necessary to match the camera's settings.

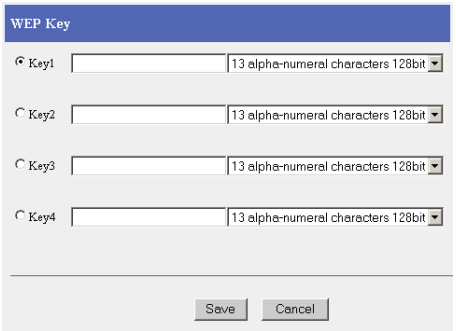
1. Click [Encryption].

2. Select from Disabled, WEP and WPA-PSK/ WPA2-PSK on the Encryption dropdown list.
- If Disabled is selected, click [Save].

<When [WEP] is selected>

3. Select from 10 hexadecimal characters 64 bit, 26 hexadecimal characters 128 bit, 32 hexadecimal characters 152 bit, 5 alpha-numerical characters 64 bit, 13 alpha-numerical characters 128 bit, and 16 alpha-numerical characters 152 bit in each of WEP key 1 to WEP key 4's dropdown lists.

4. In each of WEP key 1 to WEP key 4's blank spaces, enter the number of hexadecimal ("0"-"9", "A"-"F", or "a"-"f") or alpha-numerical characters selected in the dropdown lists, and check the WEP key number you will use.



Example

WEP key	10123456789abcdef012345abc	26 hexadecimal characters 128 bit
WEP key	20123456789abcdef0123456789abcde	32 hexadecimal characters 152 bit
WEP key	3012y	5 alpha-numerical characters 64 bit
WEP key	40123456789uvwxy	16 alpha-numerical characters 152 bit

Notes

- After restarting, the setup information will be denoted by asterisks. Before you forget it, make a note of the information and store it in a safe place.
- Enter the same WEP keys 1 - 4 into the connecting wireless devices, and select the same WEP key number as in step 4. Regarding the data entry field, see page 53.
- The encryption key is called Key Index on Windows® XP.

5. Click [Save].

6. After checking the setting information, click [Restart].

Note

The KX-HCM250 and KX-HCM270 wireless LAN headings correspond to the following headings.

40 bit password entry	5 alpha-numerical characters 64 bit
128 bit password entry	13 alpha-numerical characters 128 bit
40 bit key entry	10 hexadecimal characters 64 bit
128 bit key entry	26 hexadecimal characters 128 bit

Data Entry Field

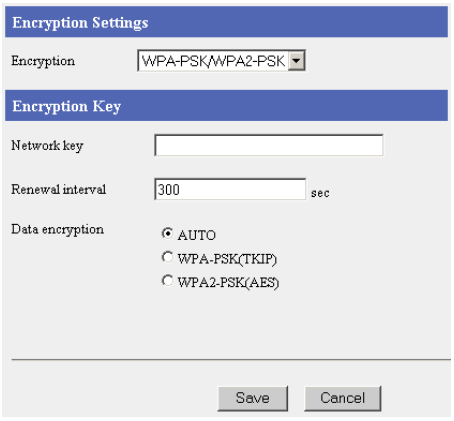
Encryption Settings	Select from Disabled, WEP, and WPA-PSK/WPA2-PSK. The method with the highest security is WPA-PSK/WPA2-PSK, followed by WEP, then Disabled. (Factory Default is WEP.)
WEP Key	Safety increases from 64 bit to 128 bit to 152 bit, but as the safety increases the data speed is reduced slightly. In Windows XP 64 bit is displayed as 40 bit(10 digits), and 128 bit is displayed as 104 bit(26 digits). (Alpha-numerical 13 characters 128 bit in WEP Key 1 is selected in factory default.)

Note

When modifying the encryption setup of this product after a wireless camera etc. has been registered automatically, it is necessary to match the wireless camera's settings.

<When [WPA-PSK/WPA2-PSK] is selected>

3. For the Network key, enter between 8 and 63 alphanumeric characters, or 64 hexadecimal characters.



Notes

- Setup details are displayed as * (asterisks) after restarting this product. Always take a memo of your setup details and keep it in a safe place.
- Set the same network key for wireless devices connected to this product. See page 54 for details about the data entry fields.
- The renewal interval is only applicable when AUTO or WPA-PSK(TKIP) is selected.

4. Set the Renewal interval and Data encryption.

5. Click [Save].

6. After checking the setting information, click [Restart].

Data Entry Field

Encryption	Select from Disabled, WEP, and WPA-PSK/WPA2-PSK. The method with the highest security is WPA-PSK/WPA2-PSK, followed by WEP, then Disabled. (Factory Default is WEP.)
Network key	Enter between 8 and 63 alphanumeric characters, or 64 hexadecimal characters. When encrypting, it is necessary to set the same network key on the device receiving the data. The set network key is only displayed once, so make a note of it if necessary.
Renewal interval	Set the interval for refreshing the encryption key. • Set a value between 30 and 604800 seconds. 604800 seconds is the equivalent of one week.
Data encryption	Select from WPA-TSK(TKIP), and WPA2-PSK(AES), and AUTO. • **WPA-PSK(TKIP)** TKIP can prevent WEP key analogy, spoofing and data falsifying, by dynamically changing the WEP key, and has better security than WEP. • **WPA2-PSK(AES)** AES is a next generation encryption method appointed by the National Information System for Science and Technology (NIST), and has better security than TKIP. • **AUTO** Allows this product to switch between TKIP and AES automatically, to match the terminal.

Notes

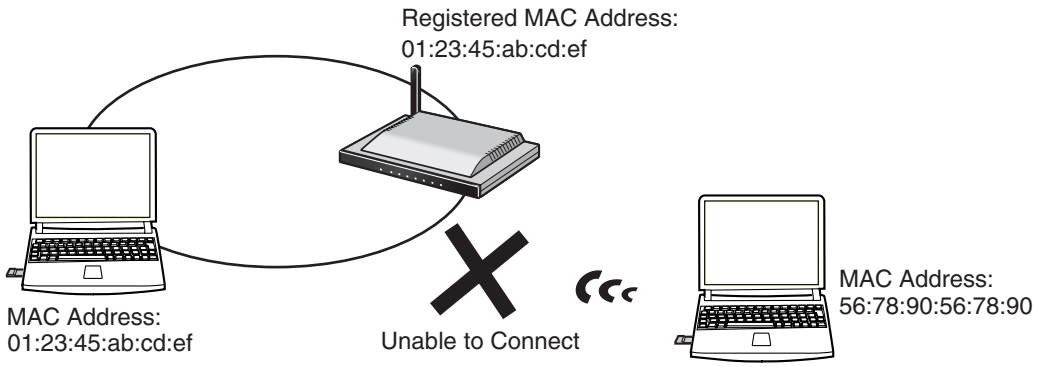
- When modifying the encryption setup of this product after a wireless camera etc. has been registered automatically, it is necessary to match the wireless camera's settings.
- When this product is using WPA-PSK(TKIP), if connected wireless devices have the same network key, they may be able to connect to this product using either the TKIP or AES encryption.

MAC Address Filtering

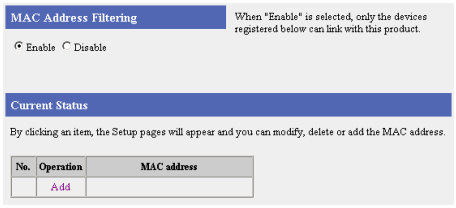
PCs that are not registered with this product cannot connect to this product. On the LAN card of each PC, a MAC address is registered, which is specific to that LAN card. If that MAC address is registered in MAC Address Filtering, only the PC with that MAC address can connect. To check the MAC address of your PC see Checking your PC's IP Address and MAC Address. (see page 132)

Note

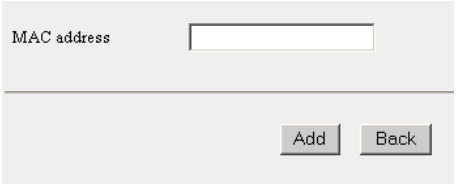
See the Panasonic Support Website (http://panasonic.co.jp/pcc/products/en/netwkcam/) for more details about Panasonic's wireless cameras.



1. Click [MAC Address Filtering].
2. Click Add under the Operation heading.


MAC Address Filtering
When "Enable" is selected, only the devices registered below can link with this product.
Enable
Disable
Current Status
By clicking an item, the Setup pages will appear and you can modify, delete or add the MAC address.
No.
Operation
MAC address
Add

3. Enter the MAC Address in the data entry field.
   - Enter two numbers or letters such as A-F (a-f) each time, separated by a : (e.g. 01:23:45:ab:cd:ef).



4. Click [Add].
5. Check Enable under MAC Address Filtering.
6. Click [Save].
7. After checking the setting information, click [Restart].

New settings are saved.
It is necessary to restart this product to complete the setting.
If you want to restart later, click the restart button on the restart page.
If you want to restart it immediately, click the restart button below.
Restart

3.1.8 Using DynamicDNS

DynamicDNS can be used to view the image from the Internet.

Using Viewnetcam.com service

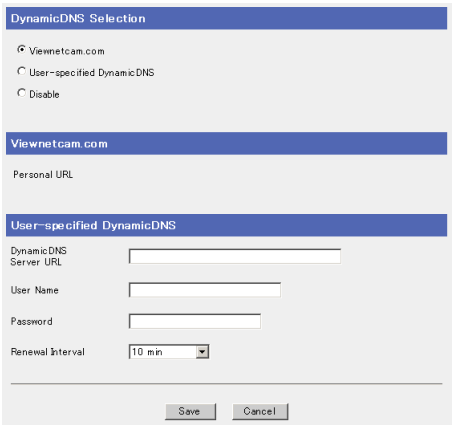
Viewnetcam.com will allow you to create a personalized web address (for example, bob.viewnetcam.com) at which your Camera Portal site can always be found on the Internet. Follow the steps below to register with the Viewnetcam.com service.

Notes

- Viewnetcam.com is a free service.
- When connecting to the Internet using a Static connection, access the camera portal using the IP address registered in this product's [Basic Setup]. It is not necessary to register for the Viewnetcam.com service.

1. Click [DynamicDNS] on the setup page.

2. Select Viewnetcam.com.



Note

When the camera is already registered for the Viewnetcam.com service, do not perform registration again.

3. Click [Save].

4. When [Restart] is displayed on the Setup Page, click it.

- The top page is displayed.

New settings are saved.
It is necessary to restart this product to complete the setting.
If you want to restart later, click the restart button on the restart page.
If you want to restart it immediately, click the restart button below.
Restart

5. Click Setup.

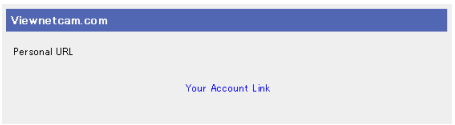
- The setup page is displayed.

6. Click [DynamicDNS].

- The Viewnetcam.com website is displayed.

Note

It may take up to 30 minutes for the Personal URL and Your Account Link to be displayed.



7. Click Your Account Link.

8. By following the Viewnetcam.com registration instructions, you can register this product with Viewnetcam.com.

9. Enter the URL displayed in Personal URL into the web browser of a PC that is connected to the Internet.

(e.g. "**http://camXXXX.viewnetcam.com:80**")

- The camera portal is displayed.

Panasonic
ideas for life
Viewnetcam.com
Your Personal Web Address for your Panasonic Network Cameras
Please enable cookies.
Home
How does it works?
How can I use it?
How do I update the firmware?
How do I register?
My Account
FAQ
Support
Registration - Welcome to Viewnetcam.com ! -
Viewnetcam.com provides remote monitoring service for your Panasonic Network Camera products. This service is free of charge.
Please start the registration to make your Panasonic Network Camera accessible from the internet by domain name.
If you have registered Panasonic Network Camera in the past, Enter your registered email address and your password.
E-mail address :
Password :
>> Next
Forgot password?
If you are new, Please start the new registration.
>> New Registration
Terms of use
Copyright (C) 2004 Matsushita Electric Industrial Co., Ltd. All Rights Reserved.

Note

The Personal URL can be used after registering with the Viewnetcam.com service.

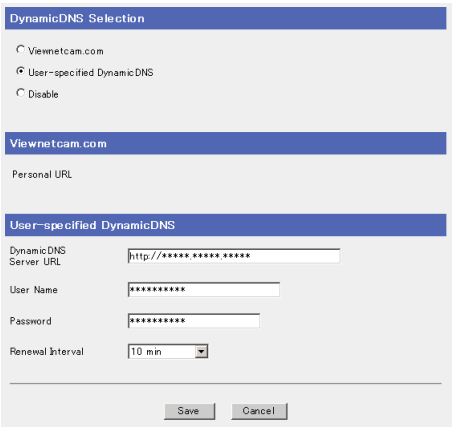
Using User-specified DynamicDNS

When you use the user-specified DynamicDNS service other than the Viewnetcam.com service, follow the steps below after registering with the ISP providing that DynamicDNS service.

Notes

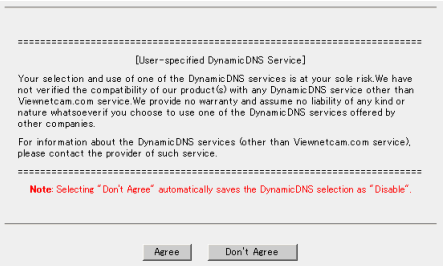
- We do not guarantee or confirm any camera operations related to the user-specified DynamicDNS services other than the Viewnetcam.com service. Therefore, you are responsible for the damages or troubles related to the user-specified DynamicDNS services.
- When using the user-specified DynamicDNS service other than the Viewnetcam.com services, confirm the operational conditions of the service. Consult with your ISP about the use or setup of the user-specified DynamicDNS service.
- When connecting to the Internet using a Static connection, access the camera portal using the IP address registered in this product's [Basic Setup]. It is not necessary to register for the user-specified DynamicDNS.

1. Click [DynamicDNS] on the setup page.
2. Select User-specified DynamicDNS.
3. Enter the URL specified by the ISP of the DynamicDNS in the DynamicDNS Server data field.
4. When the ISP specifies user name and password, enter them in the data field.
5. Select the renewal interval.



6. Click [Save].

7. After you agree with the contents in the [User-specified DynamicDNS], click [Agree].


[User-specified DynamicDNS Service]
Your selection and use of one of the DynamicDNS services is at your sole risk.We have not verified the compatibility of our product(s) with any DynamicDNS service other than Viewnetcam.com service.We provide no warranty and assume no liability of any kind or nature whatsoever if you choose to use one of the DynamicDNS services offered by other companies.
For information about the DynamicDNS services (other than Viewnetcam.com service), please contact the provider of such service.
Note: Selecting "Don't Agree" automatically saves the DynamicDNS selection as "Disable".
Agree
Don't Agree

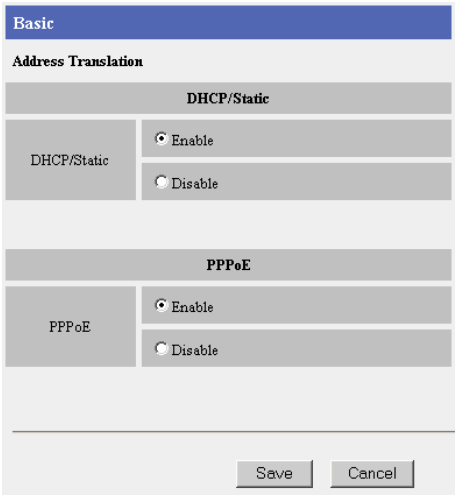
8. When [Restart] is displayed on the setup page, click it.

3.2 Using Advanced Setup

3.2.1 Accessing this Product from the Internet

The address translation page allows you to perform detailed settings in order to translate the WAN (Internet) side's global address and the private address, and access this product's network from the Internet. Set these when enabling the IP masquerade function and the port forwarding function used, for example, when starting up a mail server. When using applications that support UPnP™ (Windows/ MSN® Messenger etc.), see pages 82 and 119.

1. Click [Address Translation] on the setup page.
2. Select Enable or Disable.



3. When setup is complete, click [Save].
   - The entered information is saved.
4. When [Restart] is displayed on the setup page, click it.

Note

When performing address translation, set up the network for all PCs connected to this product, and restart the PC.

Data Entry Field

DHCP/Static	Set up when the IP masquerade and port forwarding functions are enabled. When using these functions, check [Enable].
PPPoE	Set up when the IP masquerade and port forwarding functions are enabled. When using these functions, check [Enable].

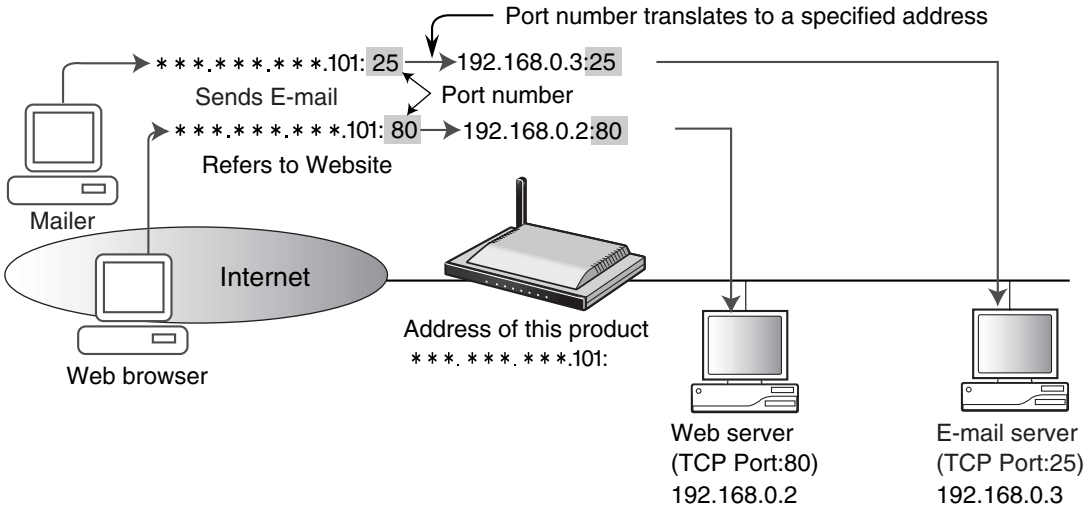
Address Translation

Port Forwarding

When data is sent from a PC on the WAN (Internet) side to the LAN (Home) server using an application, a packet is sent out to this product. The packet contains a port number used by the application, and is forwarded to a specified PC. In order to use this port forwarding function, verify which port number the application uses, enter it into the forwarding port no. entry field, and the enter the applicable PC's IP address into the forwarding IP address entry field.

Regarding principal applications and port numbers

Web server: TCP No. 80, FTP server: TCP No. 20 and No. 21
Telnet: TCP No. 23, SMTP server: TCP No. 25, POP3 server: TCP No. 110



Notes

- When installing a separate server on the LAN (Home) side, it is necessary to give it a different port number from the port number for the camera portal of this product (factory default: 80). Modify the port number for the camera portal of this product in Options. (see page 77)
- Up to 16 settings can be registered.

Example:

When making a website accessible by starting up a web server on a PC with a private address of 192.168.0.2, enter the TCP protocol, port number:80 (HTTP service port number), and 192.168.0.2 (private address).
When starting up a mail server on a PC with a private address of 192.168.0.3, enter the TCP protocol, port number:25 (HTTP service port number), and 192.168.0.3 (private address).

Example:

No.	Operation	Entry	Protocol	Forwarding Port No.	Forwarding IP Address
1	Modify/Delete	Enable	TCP	80	192.168.0.2
2	Modify/Delete	Enable	TCP	25	192.168.0.3

Notes

- Set up a TCP/IP referring to Stabilizing the PC's IP Address. (see page 135)
- The device registered as the forwarding IP address in port forwarding can be accessed from the Internet through the registered protocol and port.

Data Entry Field

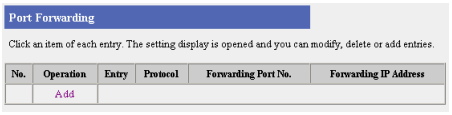
Operation	Allows you to Modify/Delete the parameters of each heading.
Entry	Select Enable or Disable. When Enable is selected, the entry functions as if set on a table (protocol, forwarding port, forwarding IP address). When Disable is selected, even if the other headings are set they will not function. They will function, however, if Enable is re-selected.
No.	Enter the entry number. Entries are processed from the lowest number.
Protocol	Select a protocol to be used when sending/receiving data over the Internet. It is possible to select from TCP, UDP, TCP & UDP, ESP, GRE and " ∗ ". " ∗ " selects all the protocols.
Forwarding Port No.	Specify a port that can be used when sending/receiving data over the Internet. Specify a forwarding port between 0 and 65535. • When you only want to use one port, enter that port number. • When entering a range, enter "-" in between the numbers. For example, when you want to use port numbers 2000 to 3000, enter "**2000-3000**". The number on the left should be lower than the number on the right.
Forwarding IP Address	Set the private address for the PC(s) connected to this product. Data from the Internet will be sent under this IP address. Stabilize this IP address on compatible PCs.

Note

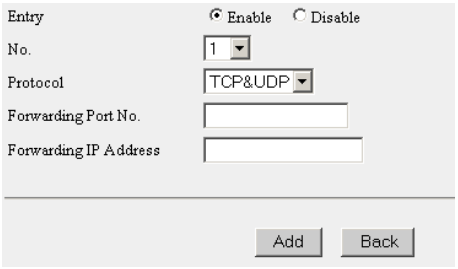
When setting up the table, there is a possibility of illegal access to the forwarding port from the Internet. For safety, only set it when required.

How to Add Entries

1. Click Port Forwarding on the Address Translation page.



2. Click Add under the Operation heading.
- The port forwarding registration page is displayed.



3. Under each heading set Entry, No., Protocol, Forwarding Port No., Forwarding IP Address.
- If Enable is checked in Entry, the specified entry is enabled. If Disable is checked, the entry will not function but the settings will not be deleted to make it easier to set up next time.
- Regarding the other headings, see the data entry field. (see page 62)

4. Click [Add].
- The port forwarding page is displayed, and the added information field will be highlighted in orange.

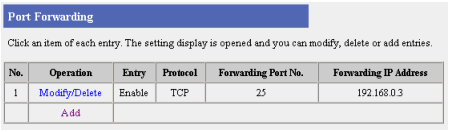
5. Click [Save].
- The restart window indicating that setup is complete is displayed.

New settings are saved.
It is necessary to restart this product to complete the setting.
If you want to restart later, click the restart button on the restart page.
If you want to restart it immediately, click the restart button below.
Restart

6. Click [Restart].

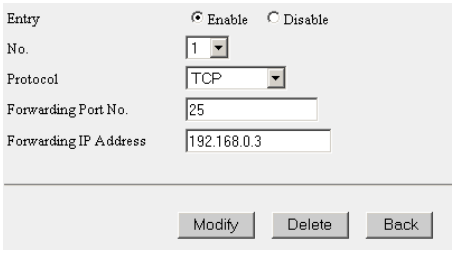
How to Modify/Delete Entries

1. Click Port Forwarding on the Address Translation page.



2. Select the No. you want to modify or delete in port forwarding, and click Modify/Delete under the operation heading.

- The port forwarding registration page is displayed.

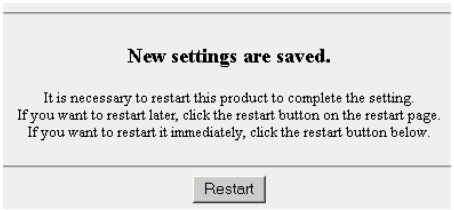


3. When you want to modify the settings, click [Modify], when you want to delete the settings, click [Delete].

- The port forwarding page is displayed.
- After modification, the modified information field will be highlighted in orange and the settings will have changed.
- After deletion, the deleted information field will be highlighted in orange and Unsaved Deletion is displayed.

4. Click [Save].

- The restart window indicating that setup is complete is displayed.


New settings are saved.
It is necessary to restart this product to complete the setting.
If you want to restart later, click the restart button on the restart page.
If you want to restart it immediately, click the restart button below.
Restart

5. Click [Restart].

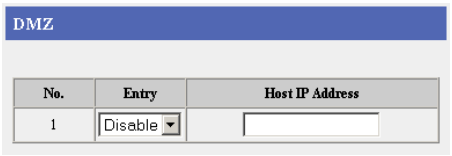
The DMZ Function

The DMZ (De-militarized Zone) function allows destination unknown packets sent from the WAN (Internet) side to the LAN (Home) side, to be forwarded to an IP address specified in the DMZ function's settings. Packets sent by the DMZ function are forwarded to the registered IP address after being passed through all the security filters.

DMZ Function

1. Click Port Forwarding on the Address Translation page.

2. Select Enable from the drop-down list in Entry, and enter the forwarding destination IP address into the DMZ function's Host IP Address field.



Notes

- The IP address registered at the forwarding destination should be the same as the IP address on the LAN.
- The DMZ function on this product can forward data to an IP address of a device connected to the LAN (Home) side using port forwarding. The IP address filters registered at the forwarding destination are disabled. The DMZ function of this product does not split the network into segments. Therefore, in the unlikely event that the forwarding destination IP address is attacked, there is a chance that other devices connected to the LAN side have also been attacked. Bear this in mind when using this system and take safety precautions.
- When using the DMZ function, set Address Translation to Enable. (see page 60)
- The DMZ function is not compatible with the Camera Portal (No.TCP/80[Default]), Setup (No.TCP/8080[Default]), the PPTP server function (No.TCP/1723, GRE) and IPsec function (No.UDP/500, ESP). Also, when IPv6 Tunneling Connection or IPv6 6to4 Connection is being used, the IPv6 protocol (Protocol No. 41) is not compatible with the DMZ function.

3. When setup is complete, click [Save].

- The entered information is saved.

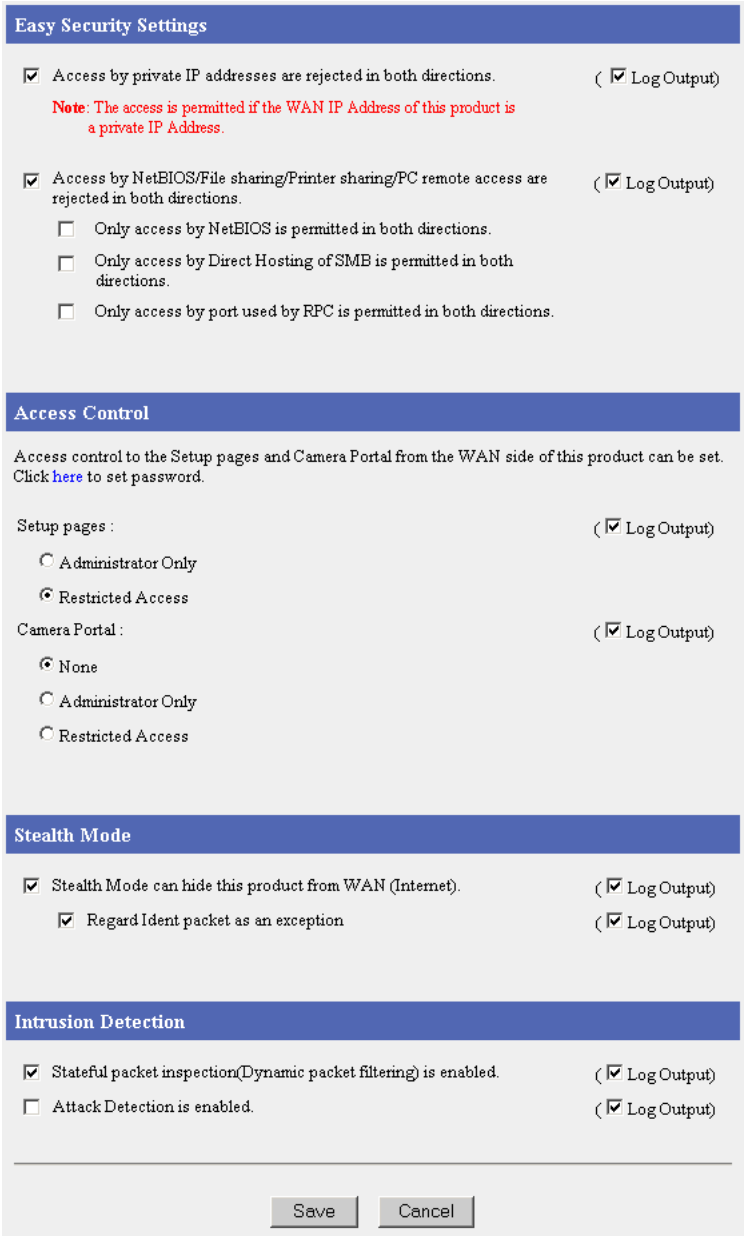
Note

When saving, do not cut the power supply. If cut, saving might not be completed successfully.

4. When [Restart] is displayed on the setup page, click it.

3.2.2 Improving Security

This function allows you to limit access to this product and set up filtering easily. When performing security setup, a filtering log is saved in the default settings. The saved log is displayed as a three-character abbreviation. (see page 67)


Easy Security Settings
Access by private IP addresses are rejected in both directions.
(Log Output)
Note: The access is permitted if the WAN IP Address of this product is a private IP Address.
Access by NetBIOS/File sharing/Printer sharing/PC remote access are rejected in both directions.
(Log Output)
Only access by NetBIOS is permitted in both directions.
Only access by Direct Hosting of SMB is permitted in both directions.
Only access by port used by RPC is permitted in both directions.
Access Control
Access control to the Setup pages and Camera Portal from the WAN side of this product can be set.
Click here to set password.
Setup pages :
(Log Output)
Administrator Only
Restricted Access
Camera Portal :
(Log Output)
None
Administrator Only
Restricted Access
Stealth Mode
Stealth Mode can hide this product from WAN (Internet).
(Log Output)
Regard Ident packet as an exception
(Log Output)
Intrusion Detection
Stateful packet inspection(Dynamic packet filtering) is enabled.
(Log Output)
Attack Detection is enabled.
(Log Output)
Save
Cancel

Data Entry Field

Easy Security Settings	It is possible to easily set up firewalls, which appear frequently, and are very important in terms of security. The default settings are oriented to the highest possible level. Only change them if essential.
• Access by private IP addresses are rejected in both directions.	Display when saving log: P-P When the source of an incoming (from WAN side) and destination of an outgoing (to WAN side) packet is a private address, access to this product is prohibited. In factory default settings Access by private IP addresses are rejected in both directions and Log Output are both checked.
• Access by NetBIOS/ File sharing/Printer sharing/PC remote access are rejected in both directions.	Display when saving log: SHR Prohibits the access in both ways of packets sent/received when files or printers are shared on Windows. In factory default settings Access by NetBIOS/File sharing/Printer sharing/PC remote access are rejected in both directions and Log Output are both checked.
Access Control • Setup pages	Settings to limit access to this product from the WAN side. Display when saving log: W-C It is possible to select either Administrator Only or Restricted Access for access to Setup from the WAN side. In factory default settings Restricted Access and Log Output are both checked.
• Camera Portal	Display when saving log: W-P It is possible to select either None, Administrator Only or Restricted Access for access to Camera Portal from the WAN side. In factory default settings None and Log Output are both checked.
Stealth Mode • Stealth Mode can hide this product from WAN (Internet).	Display when saving log: STL It is possible to set this product to not respond to Pings etc. from the WAN (Internet) side. Therefore it can escape the attacker's existence verification produced by Pings etc. It will also not respond to UDP/ TCP port scans. In factory default settings Stealth Mode can hide this product from WAN (Internet) and Log Output are both checked.
• Regard Ident packet as an exception	Display when saving log: STL (Ident) When clients try to send/receive E-mail, There is E-mail server that authenticates E-mails to/from clients. This authentication uses recognition protocol, which uses TCP port number 113. The authentication level is relatively low so there are not many cases where clients are unable to send/receive E-mails. In factory default settings Regard the Ident Packet as an Exception and Log Output are both checked.
Intrusion Detection	When using the intrusion detection function, check the field under each heading.
• Stateful packet inspection (Dynamic packet filtering) is enabled	Display when saving log: SPI If a packet being received from the WAN side is inspected, and judged to be a corrupt packet, it is intercepted. By comparing the packet to static filtering (packet filtering through header information), Internet data can be sent more safely. In factory default settings Stateful packet inspection (Dynamic packet filtering) is enabled and Log Output are both checked.

• Attack Detection is enabled	Display when saving log: DoS Harmful data from the WAN side is detected, and the packet is intercepted. A detection record is noted in the log. The following types of attacks can be detected: • TCP Scan • UDP Scan • ICMP Echo

Notes

- If the log output heading is unchecked, a log will not be recorded.
- In order to improve security, it is necessary to manage your current software and update firmware as appropriate.

Priority of Security Functions

In order for this product to combat various types of illegal access from the Internet, it is equipped with the following security functions:
[Prioritization (top to bottom)]

- Packet Filtering (see page 69)
- Easy Security Settings (see page 66)
- Stealth Mode (see page 67)

These functions are executed in the above order. At each level the packet is either passed or intercepted.

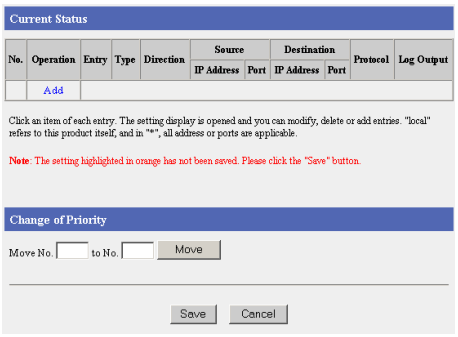
Note

When using the DMZ function (see page 65), the security function cannot be executed for DMZ terminal packets.

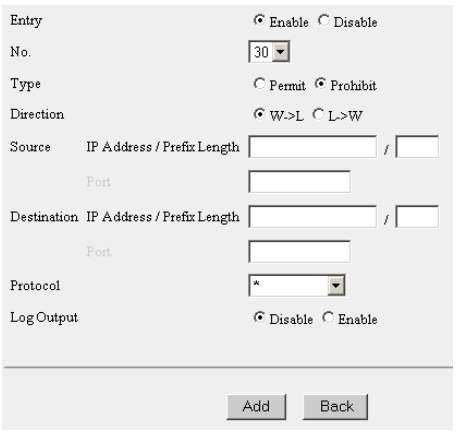
Packet Filtering

By specifying the IP address, port and protocol parameters, it is possible to either pass or intercept IP packets that are being received. If the parameters are set effectively they can be used as a security measure. Filtering is processed from the smallest entry no. up. For an explanation of each heading in filtering, see below.

1. Click [Packet Filtering] on the security setup page.
2. Click Add under the Operation heading.



3. Set the necessary headings and click [Add].
4. When setup is complete, click [Save].
   - The entered information is saved.



5. When [Restart] is displayed on the setup page, click it.

Notes

- You must click [Save] after setting the filtering parameters.

Data Entry Field

No.	Select an entry no. between 1 and 64. Packet filtering is processed from the smallest entry no. up. If an entry is already registered, it will be overwritten by the new entry.
Operation	Click Add to add a new filtering setting. To modify or delete a filtering setting click Modify/Delete. The setup page will open and you can add, modify or delete settings by entering the data and clicking the appropriate button.
Entry	Enable or Disable this entry.

Type	Select Permit (if it conforms to the parameters it will be passed) or Prohibit (if it conforms to the parameters it will be intercepted).
Direction	Select W → L (filtering when receiving from WAN) or L → W (filtering when sending to WAN).
Source IP Address/Prefix Length	Set the packet source IP address to be filtered. • When specifying only 1 IP address, enter the IP address and its subnet prefix length. • When specifying an IP address range, enter the network address in the IP address field, and the network prefix number in the prefix length field. For example, when specifying an network address of 192.168.0.0/16, enter 192.168.0.0 in the IP address field, and 16 in the prefix length field. • If " ∗ " is entered in the IP address field, all packets are filtered. **Note** When specifying an IP address range, even if this product's IP address is included in the range, this product will not be filtered. When you want to filter this product, it is necessary to enter " ∗ " or the code for this product (local) in the IP address data field.
Source Port	Set the packet source port to be filtered. • When using only 1 port, enter the port number. • When entering a range, enter "-" in between the numbers. For example, when you want to use port numbers 2000 to 3000, enter "**2000-3000**". The number on the left should be lower than the number on the right. • If " ∗ " is entered, all packets are filtered.
Destination IP Address/Prefix Length	Set the packet destination IP address to be filtered. Entry is the same as for the source IP address. When you want to specify this product, enter "**local**".
Destination Port	Set the packet destination port number to be filtered. Entry is the same as for the Source Port.
Protocol	Select a protocol to be used when sending/receiving data. It is possible to select from TCP, UDP, TCP & UDP, ICMP, ESP, GRE and " ∗ ". " ∗ " selects all the protocols.
Log Output	Set whether to display the temporarily saved packet information on the [Filtering Log].

Modifying or Deleting Filtering Headings

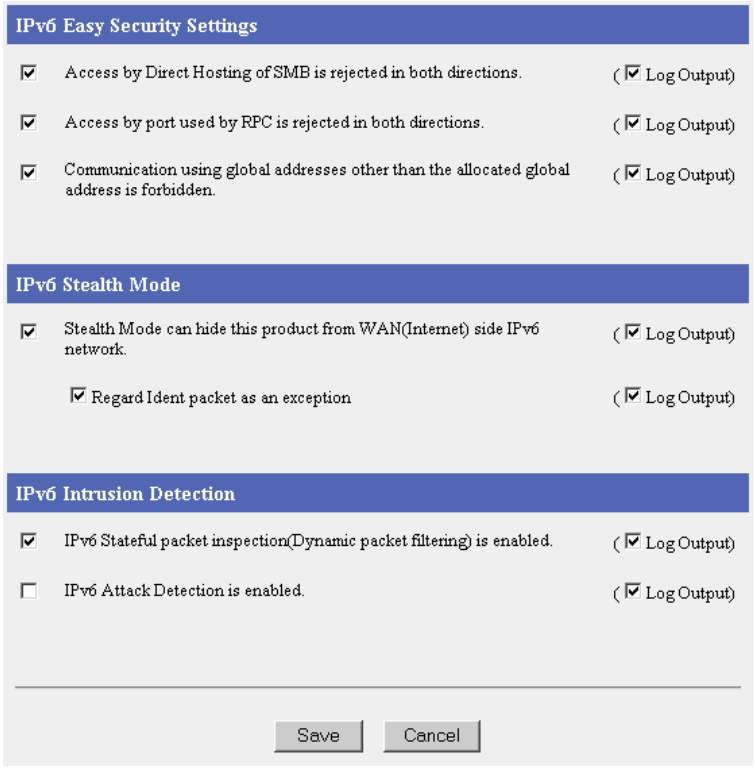
1. Click Packet Filtering on the security setup page.
2. Click Modify/Delete under the operation heading of the filter you want to modify or delete from the filtering parameters list.
3. Click [Modify] to modify, or [Delete] to delete the selected heading.
4. When setup is complete, click [Save].
   - The entered information is saved.
5. When [Restart] is displayed on the setup page, click it.

Changing the Priority of Filtering Headings

Packet filtering is processed starting from the smallest entry no. To change the priority of filtering headings, on Change of Priority on the filtering setup page, enter the heading entry no. you want to move in the left data field, the destination entry no. in the right data field, and click [Move]. Then, click [Save] and when [Restart] is displayed on the setup page, click it.

3.2.3 Improving IPv6 Security

This function allows you to limit IPv6 connection access to this product and set up filtering easily. In Factory Default Settings, a filtering log is saved when security setup is performed. The saved log is displayed as a three-character abbreviation. (see below)


IPv6 Easy Security Settings
Access by Direct Hosting of SMB is rejected in both directions.
(Log Output)
Access by port used by RPC is rejected in both directions.
(Log Output)
Communication using global addresses other than the allocated global address is forbidden.
(Log Output)
IPv6 Stealth Mode
Stealth Mode can hide this product from WAN(Internet) side IPv6 network.
(Log Output)
Regard Ident packet as an exception
(Log Output)
IPv6 Intrusion Detection
IPv6 Stateful packet inspection(Dynamic packet filtering) is enabled.
(Log Output)
IPv6 Attack Detection is enabled.
(Log Output)
Save
Cancel

Data Entry Field

IPv6 Easy Security Settings • Access by Direct Hosting of SMB is rejected in both directions. • Access by port used by RPC is rejected in both directions.	It is possible to easily set up firewalls, which appear frequently, and are very important in terms of security. The default settings are oriented to the highest possible level. Only change them if essential. Display when saving log: SHR Rejects access in both directions by Direct Hosting of SMB. In factory default settings Access by Direct Hosting of SMB is rejected in both directions and Log Output are both checked. Display when saving log: SHR Rejects access in both directions by the port used by RPC. In factory default settings Access by port used by RPC is rejected in both directions and Log Output are both checked.

• Communication using global addresses other than the allocated global address is forbidden.	Display when saving log: GOR Prohibits communication using global addresses other than the allocated global address. The allocated global address contains an IPv6 side WAN address, and IPv6 addresses which have a LAN side prefix/prefix length. In factory default settings Communication using global addresses other than the allocated global address is forbidden and Log Output are both checked.
IPv6 Stealth Mode • Stealth Mode can hide this product from WAN (Internet) side IPv6 network.	Display when saving log: STL It is possible to set this product to not respond to IPv6 Pings etc. from the WAN (Internet) side. Therefore it can escape the attacker's existence verification produced by IPv6 Pings etc. It will also not respond to UDP/TCP port scans. In factory default settings Stealth Mode can hide this product from WAN (Internet) side IPv6 network and Log Output are both checked.
• Regard Ident packet as an exception	Display when saving log: STL (Ident) When clients try to send/receive E-mail, There is E-mail server that authenticates E-mails to/from clients. This authentication uses recognition protocol, which uses TCP port number 113. The authentication level is relatively low so there are not many cases where clients are unable to send /receive E-mails. In factory default settings Regard Ident packet as an exception and Log Output are both checked.
IPv6 Intrusion Detection	When using the intrusion detection function, check the box next to each heading.
• IPv6 Stateful packet inspection (Dynamic packet filtering) is enabled.	Display when saving log: SPI If a packet being received from the WAN side is inspected, and judged to be a corrupt packet, it is destroyed. By comparing the packet to static filtering (packet filtering through header information), Internet data can be sent more safely. In factory default settings IPv6 Stateful packet inspection (Dynamic packet filtering) is enabled and Log Output are both checked.
• IPv6 Attack Detection is enabled.	Display when saving log: DoS Harmful data from the WAN side is detected, and the packet is destroyed. A detection record is noted in the log. The following types of attacks can be detected: • TCP Scan • UDP Scan • ICMP Echo

Notes

- If the log output heading is unchecked, a log will not be recorded.
- In order to improve security, it is necessary to manage your current software and update firmware as appropriate.

Priority of Security Functions

In order for this product to combat various types of illegal access from the Internet, it is equipped with the following security functions:

[Prioritization (top to bottom)]

- IPv6 Packet Filtering (see below)
- IPv6 Easy Security Settings (see page 72)
- IPv6 Stealth Mode (see page 73)

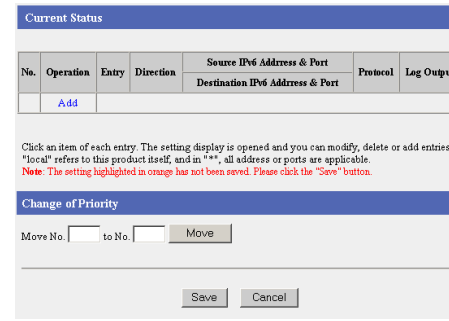
These functions are executed in the above order. At each level the packet is either passed or destroyed.

IPv6 Packet Filtering

This function allows you to filter only IPv6 packets. By specifying the IPv6 address, port and protocol parameters, it is possible to either pass or intercept IPv6 packets that are being received. If the parameters are set effectively they can be used as a security measure. Filtering is processed from the smallest entry no. up. For an explanation of each heading in filtering, see page 75.

1. Click [IPv6 Packet Filtering] on the security setup page.

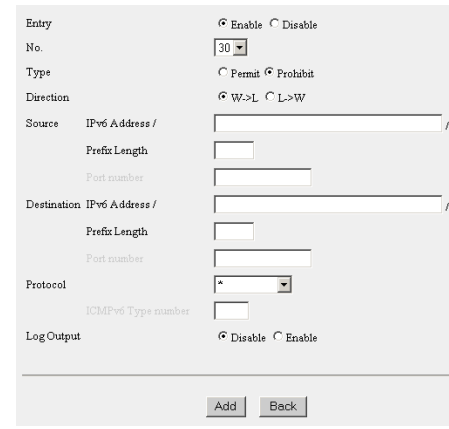
2. Click Add under the Operation heading.


Current Status
No.
Operation
Entry
Direction
Source IPv6 Address & Port
Destination IPv6 Address & Port
Protocol
Log Output
Add
Click an item of each entry. The setting display is opened and you can modify, delete or add entries.
"local" refers to this product itself, and in "*", all address or ports are applicable.
Note. The setting highlighted in orange has not been saved. Please click the "Save" button.
Change of Priority
Move No.
to No.
Move
Save
Cancel

3. Set the necessary headings and click [Add].

4. When setup is complete, click [Save].

- The entered information is saved.



5. When [Restart] is displayed on the setup page, click it.

Notes

- You must click [Save] after setting the filtering parameters.

Data Entry Field

No.	Select an entry no. between 1 and 64. Packet filtering is processed from the smallest entry no. up. If an entry is already registered, it will be overwritten by the new entry.
Operation	Click Add to add a new filtering setting. To modify or delete a filtering setting click Modify/Delete. The setup page will open and you can add, modify or delete settings by entering the data and clicking the appropriate button.
Entry	Enable or Disable this entry.
Type	Select Permit (if it conforms to the parameters it will be passed) or Prohibit (if it conforms to the parameters it will be intercepted).
Direction	Select W → L (filtering when receiving from WAN) or L → W (filtering when sending to WAN).
Source IPv6 Address/Mask Length	Set the source IPv6 address of the packet to be filtered. • When specifying only 1 IPv6 address, set the prefix length to 128. For example, when setting 2002:C0A8:1234:0123:4567:89ab:cdef:0123/128, enter 2002:C0A8:1234:0123:4567:89ab:cdef:0123 into the IPv6 address field and 128 into the prefix length field. • When specifying an IPv6 address range, usually set the prefix to a value less than 64. For example, when setting 2002:C0A8:1234::/48, enter 2002:C0A8:1234:: into the IPv6 address field and 48 into the prefix length field. • If " ∗ " is entered in the IPv6 address field, all packets are filtered. **Note** When specifying an IPv6 address range, even if this product's IPv6 address is included in the range, this product will not be filtered. When you want to filter this product, it is necessary to enter " ∗ " or the code for this product (local) in the IPv6 address data field.
Source Port	Set the source port of the packet to be filtered. • When using only 1 port, enter the port number. • When entering a range, enter "-" in between the numbers. For example, when you want to use port numbers 2000 to 3000, enter "**2000-3000**". The number on the left should be lower than the number on the right. • If " ∗ " is entered, all packets are filtered.
Destination IPv6 Address/Mask Length	Set the destination IPv6 address of the packet to be filtered. Entry is the same as for the source IPv6 address. When you want to specify this product, enter "**local**".
Destination Port	Set the destination port number of the packet to be filtered. Entry is the same as for the Source Port.
Protocol	Select a protocol to be used when sending/receiving data. It is possible to select from TCP, UDP, TCP & UDP, ICMPv6, ESP, and " ∗ ". " ∗ " selects all the protocols. ICMPv6 can set the type number. **Note** When selecting ICMPv6, the ICMPv6 type number may cause problems to the network.
Log Output	Set whether to display the temporarily saved packet information on the [Filtering Log].

Modifying or Deleting Filtering Headings

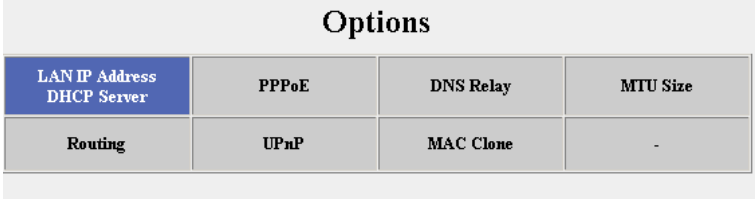
1. Click IPv6 Packet Filtering on the security setup page.
2. Click Modify/Delete under the operation heading of the filter you want to modify or delete from the filtering parameters list.
3. Click [Modify] to modify, or [Delete] to delete the selected heading.
4. When setup is complete, click [Save].
   - The entered information is saved.
5. When [Restart] is displayed on the setup page, click it.

Changing the Priority of Filtering Headings

Packet filtering is processed starting from the smallest entry no. To change the priority of filtering headings, on Change of Priority on the filtering setup page, enter the heading entry no. you want to move in the left data field, the destination entry no. in the right data field, and click [Move]. Then, click [Save] and when [Restart] is displayed on the setup page, click it.

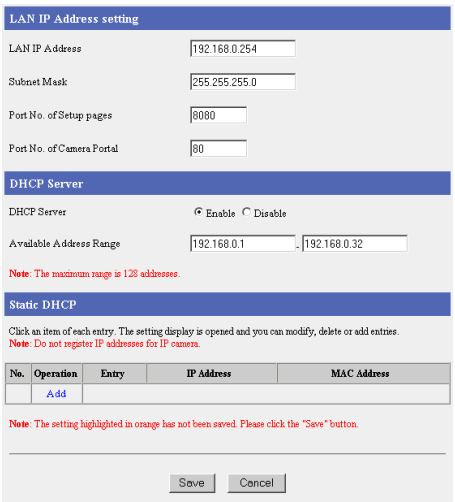
3.2.4 Using Options

The options setup page allows you to set LAN (Home) settings and WAN (Internet) access settings. It is possible to set the following 7 headings: LAN IP Address DHCP Server, PPPoE, DNS Relay, MTU Size, Routing, UPnP, and MAC Clone.



Only modify Options when it is essential. Take the following steps to modify Options.

1. Click [Options] on the setup page.
   - See next page for details of each heading.
2. Select a setup heading at the top of the page.
3. Enter the modified data in the data entry field.
   - To return to the original settings, click [Cancel].
4. When setup is complete, click [Save].
   - The entered information is saved.



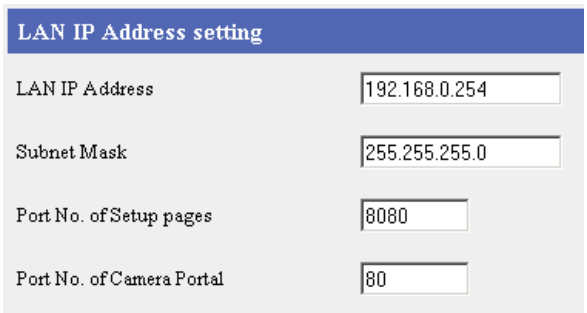
5. When [Restart] is displayed on the setup page, click it.

Notes

- When modifying options, set the PC(s) connected to this product accordingly, then restart the PC(s).

LAN IP Address DHCP Server

LAN IP Address setting



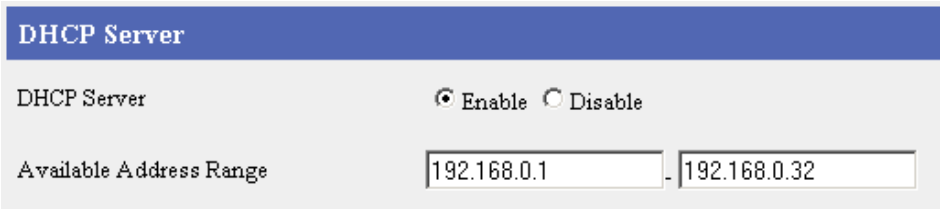
Functions

LAN IP Address	You can enter the LAN (Home) side's IP address. The default factory setting is 192.186.0.254. The IP address should not overlap neither the Available Address Range in DHCP setup, the PPTP server's Available Address Range specified in PPTP Server Setup found on the basic page of VPN, or the Available Address Range specified in Automatic Setup on the Camera setup page.
Subnet Mask	Enter the LAN (Home) side subnet mask.
Port No. of Setup pages	Enter a port number for the Setup pages. Use a port number less than 65535. However, the numbers 1-1023 (excluding 80) because they are well-known ports, and 53, 1723, and 10000 because they are used by this product, cannot be used.
Port No. of Camera Portal	Enter a port number for the Camera Portal. Use a port number less than 65535. However, the numbers 1-1023 (excluding 80) because they are well-known ports, and 53, 1723, and 10000 because they are used by this product, cannot be used.

Note

When changing the LAN side network, for example, to 192.168.1.254, change the Available Address Range in Automatic Setup in Camera accordingly.

DHCP Server



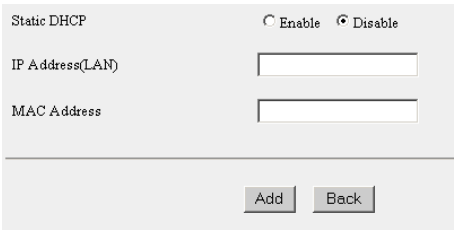
Devices connected to the LAN (Home) side are automatically assigned an IP address when using the DHCP server function.

DHCP Server	Devices connected to the LAN (Home) side are automatically assigned an IP address. The default setting is set to Enable. When setting IP address for all the devices connected to LAN side manually, select Disable. When modifying DHCP server settings, modify the IP addresses of each PC.
Available Address Range	When using the DHCP server function, enter the private address range in the data entry field. The maximum amount of characters is 128. Do not modify this unless necessary.

Static DHCP

The DHCP static function allows you to stabilize the IP address assigned to the PC by registering the PC's MAC address.

The window (right) is displayed by clicking Add.

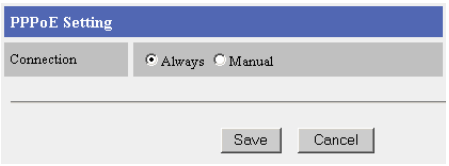


Static DHCP	Select Enable or Disable. When Enable is selected, the entry table stabilizes the IP address set in the table, on the PC with the MAC address set in the table. When Disable is selected, even if the other headings are set they will not function. They will function, however, if Enable is re-selected.
IP Address (LAN)	Enter the IP address that you want to stabilize of the corresponding PC.
MAC Address	Enter the LAN card's MAC address of the corresponding PC. Enter two numbers or letters between A-F (a-f) each time, separated by a colon, ":" (e.g. 01:23:45:ab:cd:ef).

PPPoE

This function allows you to connect/disconnect PPPoE connection, when using it to connect with an ISP. When the charge for Internet access is metered according to the contract with your ISP, select Manual Connection.

The window (right) is displayed by clicking PPPoE.



Always	Connected whenever the power is turned on. This is the default setting. You can disconnect manually on the PPPoE connection page. (see page 106)
Manual	Only connected when Connect is selected on the PPPoE connection page. (see page 106) To disconnect PPPoE connection, click Disconnect on the PPPoE connection page.

DNS Relay

When stabilizing the IP address of a PC connected to the LAN (Home) side, it is necessary to enter the DNS server address into the PC for it to connect to the Internet. DNS relay shortens this troublesome process. Due to DNS relay, this product can inform PCs on the LAN (Home) network of its existence like a DNS server. Regarding DNS inquiries from the LAN (Home) side, this product contacts a specified DNS server on the WAN (Internet) side, on its behalf. Then it sends the reply back to PCs on the LAN (Home) side.

The setup page is displayed by clicking DNS Relay.

Note

When connecting a DNS server to the LAN (Home) side, do not use DNS relay.

Enable	This product sends/receives data to and from PCs on behalf of a DNS server. The default is set to Enable. When stabilizing a PC's IP address, enter this product's IP address (192.168.0.254) into the PC's DNS server address field.
Disable	The DNS relay function will not work. When stabilizing a PC's IP address, enter the DNS server address into the PC's DNS server address field.

MTU Size

MTU is the largest possible packet that can be sent. The larger the value of MTU the bigger the packet can be, which is forwarded in one go. However, if the value of MTU is too big, the packet may be split, and forwarded in several parts. As a result, the forwarding speed is reduced. Usually, this product sets an appropriate MTU value automatically. Only modify it when necessary.

The setup page is displayed by clicking (MTU Size).

Note

Data speed may be vastly reduced depending on the MTU settings.

Routing

This Function allows you to set dynamic routing and static routing.

The setup page is displayed by clicking Routing.

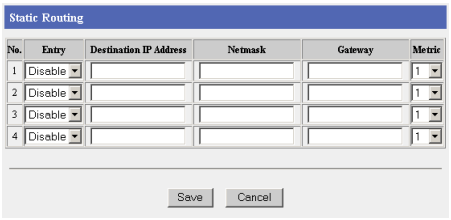
Dynamic Routing Setup

LAN	Allows you to set Send & Receive, Receive only, Send only, and Disable for path information held by this product, for RIP supporting devices on the LAN (Home) side. The default is set to Disable.
WAN	When sending path information to the WAN (Information) side, LAN side information can be seen from the outside. It is possible to select Send & Receive, Receive only, Send only, and Disable. The default is set to Disable.

Static routing

Apart from dynamic routing which is determined automatically, up to 4 stable routing destinations can be set. This allows the building of several subnetworks and the setting of a flexible routing system.

1. Click Routing in Options.
2. Set Entry, Destination IP Address, Netmask, Gateway, and Metric, in Static Routing
3. Click [Save].
   - The restart window indicating that setup is complete is displayed.



4. Click [Restart].

Data Entry Field

Entry	Specifying Enable in this heading enables the static routing setting set previously. Select Disable if you do not want to use static routing. Even if Disable is selected the entered settings will not be deleted.
Destination IP Address	Enter the IP address of the destination host or network.
Netmask	Enter the netmask for the destination IP address.
Gateway	Enter the gateway IP address.
Metric	Select the Metric value from the dropdown list. Metric is the number of routers that the packet will pass through.

Note

The destinations set in static routing are limited to the gateway IP address on this product's network. However, gateways connected to WAN side ports using DHCP or PPPoE cannot be set as a static routing forwarding destination.

UPnP™

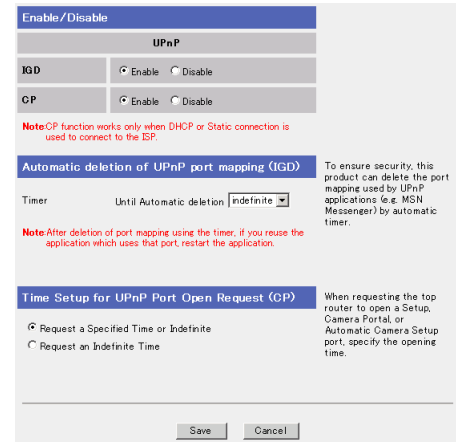
This product allows you to use UPnP™ compatible applications and UPnP™ compatible devices. The UPnP™ function is compatible with PCs that use a wired or wireless connection. Regarding the use of UPnP™ supporting applications (Windows/MSN Messenger etc.) see page 119.

1. Click UPnP in Options.

2. Set Enable/Disable for UPnP.

3. Set a time for Automatic deletion of UPnP port mapping (IGD).

- This function allows you to set a time to delete the port opened dynamically by Messenger supporting functions. Set a time (hour) between 1 and 24 hours. If Indefinite is selected, the port will not be deleted automatically. In this case, it is necessary to manually delete the port, either by restarting this product, or clicking [Delete Table] on the UPnP™ Port Mapping Table on the status page.


Enable/Disable
UPnP
IGD
Enable
Disable
CP
Enable
Disable
Note:CP function works only when DHCP or Static connection is used to connect to the ISP.
Automatic deletion of UPnP port mapping (IGD)
To ensure security, this product can delete the port mapping used by UPnP applications (e.g. MSN Messenger) by automatic timer.
Timer
Until Automatic deletion
indefinite
Note:After deletion of port mapping using the timer, if you reuse the application which uses that port, restart the application.
Time Setup for UPnP Port Open Request (CP)
When requesting the top router to open a Setup, Camera Portal, or Automatic Camera Setup port, specify the opening time.
Request a Specified Time or Indefinite
Request an Indefinite Time
Save
Cancel

4. Set the Time Setup for UPnP Port Open Request (CP).

- Set the time to open a port for forwarding a packet to a UPnP™ compatible router connected to the WAN side of this product. If Request a Specified Time or Indefinite is selected, first, a request is made to the UPnP™ compatible router for a port to be opened for a specified time, but if that request is denied, indefinite is requested. If Request an Indefinite Time is selected, indefinite is requested from the start.

Notes

- Once a port has been registered, and the deleting time set above has passed, the port will be deleted. No matter whether the application is being used or not, when the specified time is reached the port is closed.
- When using an application intermittently for over 24 hours, such as voice chat, set the timer to indefinite. It is necessary to manually delete the port either by restarting this product, or clicking Delete Table on the UPnP Port Mapping Table on the status page. (see page 110)
- You may have to set the Time Setup for UPnP Port Open Request (CP) to Request an Indefinite Time, depending upon the UPnP™ compatible router connected to the WAN side of this product.

5. When setup is complete, click [Save].

- The entered information is saved.

Note

When saving, do not cut the power supply. If cut, saving might not be completed successfully.

6. When [Restart] is displayed on the setup page, click it.

New settings are saved.
It is necessary to restart this product to complete the setting.
If you want to restart later, click the restart button on the restart page.
If you want to restart it immediately, click the restart button below.
Restart

Notes

- When modifying address translation settings, also set the PCs connected to this product, and restart the PCs.
- When setting Automatic deletion of UPnP™ port mapping to indefinite, the external port opened in UPnP™ will not close without instruction from the application. From a security perspective, when using Windows/MSN Messenger, set the timer to delete the port automatically.

  Also, when using Windows/MSN Messenger and the port is deleted by timer, shutdown Windows/MSN Messenger once first before trying to sign in again. Windows/MSN Messenger will not operate without once shutting down first.
- When this product is working under a UPnP™ supporting router connected to the WAN side, sometimes the IGD function does not work in this product's security settings, which is due to the router's specifications. Set the stealth mode settings of this product to Disable. (see page 67)

Working Under a UPnP™ Supporting Router

CP Function

The CP function allows you to control the port mapping of a UPnP™ supporting router connected to the WAN side (hereinafter known as 'Top router'). A device with this function is called a CP (Control Point). This function is enabled for cameras registered on this product.

Notes

- Even if the Top router supports UPnP™, it may not work due to the Top router's specifications.
- When the settings for filtering sent data from WAN to LAN through the Top router have been set, sometimes access from the Internet to the Camera Portal and cameras connected to the LAN side is denied. It is necessary to modify the filtering settings of the Top router.
- When the Top router web server is using port number 80, either modify the Top router settings, or change the port number of this product's web server to a number other than 80 (e.g. 8081). (see page 77)

  When changing this product's web server's port number, specify the new port number in the web browser's address bar. (e.g. "**http://WAN_side_IP_address:8081**")
- Sometimes the CP function does not work, due to the Top router's specifications.

Display of UPnP™ Related Information

UPnP™ Log

Information about port mapping performed by Windows/MSN Messenger on this product is displayed. It is necessary to set the IGD function on UPnP™ on the options page to Enable in advance.
Information about request logs performed by Windows/MSN Messenger on this product is displayed, most recent first. It can hold up to 400 logs. If 400 logs is exceeded, old logs will be deleted. Also, when this product is restarted, UPnP™ log information will be deleted.
Regarding methods of checking the UPnP™ logs, see page 112.

MAC Clone

You can clone the MAC address of your PC's network adapter onto this product.

A MAC address is a 12-digit code assigned to a unique piece of hardware for identification. Some ISPs require that you register the MAC address of your PC's network adaptor, which was connected to your cable or DSL modem during installation.

To enable MAC address cloning, enter your adaptor's MAC address in the New MAC address field, and click [Save].

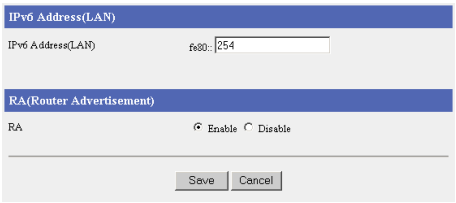
To disable MAC address cloning and the keep the default setting, click [Cancel].

3.2.5 Using IPv6 Options

This function allows you to perform detailed IPv6 settings on this product. Only modify these settings if essential. You may need specialist knowledge when performing these settings.
The options setup page allows you to set LAN (Home) settings and WAN (Internet) access settings. It is possible to set the following 3 headings: IPv6 Address(LAN)/RA, Link MTU size, and Routing.

When necessary, take the following steps to modify Options.

1. Click [IPv6 Options] on the setup page.
   - See next page for details of each heading.
2. Select a setup heading at the top of the page.
3. Enter the modified data in the data entry field.
   - To return to the original settings, click [Cancel].
4. When setup is complete, click [Save].
   - The entered information is saved.
5. When [Restart] is displayed on the setup page, click it.



Note

When modifying IPv6 options, set the PC(s) connected to this product accordingly, then restart the PC(s).

IPv6 Address(LAN) RA

IPv6 Address(LAN)

IPv6 Address(LAN)	Sets this product's LAN IPv6 link local address. The default setting is fe80::254.

RA(Router Advertisement)

RA	Sets whether to Enable or Disable the sending of RA from this product to the LAN side. Usually, it is not necessary to change this setting. The default setting is Enable.

Note

The RA is disabled when the WAN side IPv6 global address is not assigned.

Link MTU size

This function allows you set the WAN side IPv6 link MTU size. Link MTU size is the maximum packet size that can be sent within the IPv6 network segment.
The setup page is displayed by clicking Link MTU size.

IPv6 connection	You can set the IPv6 link MTU size to between 1280 and 1500 bytes. Do not change this setting unless necessary. The default setting is 1500.

Notes

- Data speed may be vastly reduced depending on the link MTU settings.
- Some set values may not be used depending on the connection type.

Routing

This function allows you to set dynamic routing and static routing.
The setup page is displayed by clicking Routing.

IPv6 Dynamic Routing

LAN	Allows you to set Send & Receive, Receive only, Send only, and Disable path information held by this product, for RIPng supporting devices on the LAN (Home) side. The default is set to Disable.
WAN	When sending path information to the WAN (Internet) side, LAN side information can be seen from the outside. It is possible to select Send & Receive, Receive only, Send only, and Disable. The default is set to Disable.

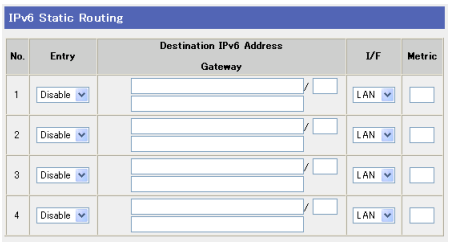
Note

Please note that this product's LAN network information is made accessible to the WAN side when either Send & Receive or Receive only are selected.

IPv6 Static Routing

This product allows you to set 4 stable gateways, as well as automatically selecting dynamic routing. Therefore it is possible to build several networks working under this product, and set a flexible routing system.

1. Click Routing in IPv6 Options.
2. Set Entry, Destination IPv6 Address, Gateway, I/F and Metric, in IPv6 Static Routing.
3. Click [Save].
   - The restart window indicating that setup is complete is displayed.
4. Click [Restart].

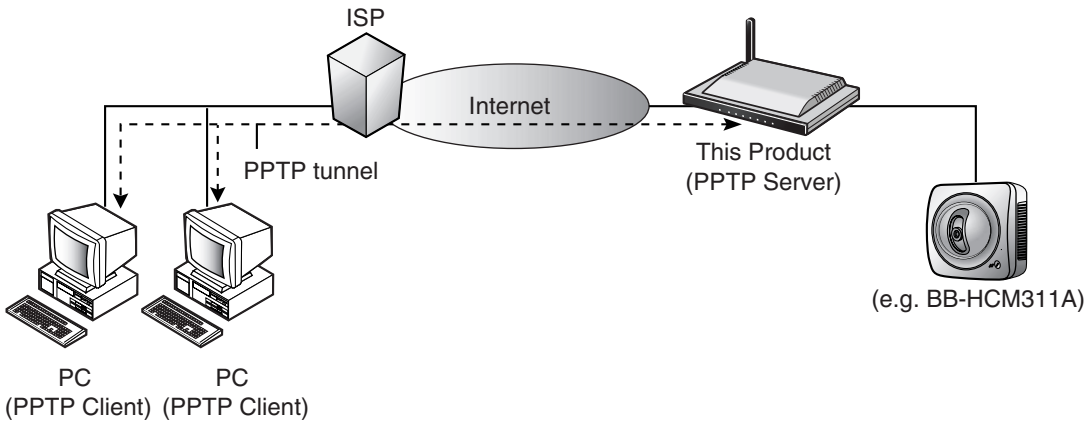


Data Entry Field

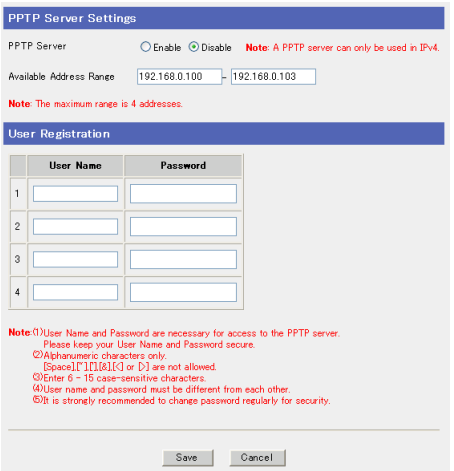
Entry	Specifying Enable in this heading enables the static routing setting set previously. Select Disable if you do not want to use static routing. Even if Disable is selected the entered settings will not be deleted.
Destination IPv6 Address	Enter the IPv6 address and prefix to be routed.
Gateway	Set the IPv6 address of the next router on the route after this product.
I/F	Set the I/F where the gateway exists.
Metric	Set the number of hops to be made to reach the Destination IPv6 Address. Enter a number between 1 and 255.

3.2.6 Using VPN (PPTP)

This product allows you to create a VPN (Virtual Private Network) using PPTP (Point-to-Point Tunneling Protocol). A VPN is private network that is as safe as an exclusive line and travels through the Internet. Using this function, camera images from PCs in far away places can be viewed safely. See page 128 when performing these settings.



1. Check Enable by PPTP Server.
2. Enter the User Name and Password and click [Save].
   - The restart window indicating that the user name and password have been set is displayed.
3. Click [Restart].
   - After the window that indicates that this product will restart, the top page is displayed.



Data Entry Field

PPTP Server	Select Enable or Disable.
Available Address Range	An IP address is assigned from the PPTP server when connected. The maximum available address range is 4. It should not overlap the IP address used in DHCP (see page 77). Factory default is set to 192.168.0.100 - 192.168.0.103.
User Name/Password	Enter a user name and password. 4 sets can be registered.

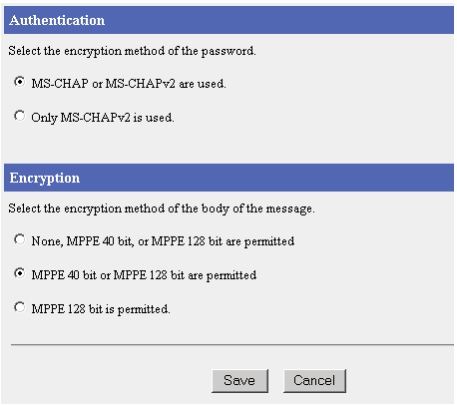
Note

The PPTP client connecting to this product's PPTP server only supports Windows XP or Windows 2000 PPTP clients.

Options

This function allows you to set up an authentication method and encryption method.

1. Check MS-CHAP or MS-CHAPv2 are used; or Only MS-CHAPv2 is used, in Authentication Method Setup.
2. Check either None, MPPE 40 bit or MPPE 128 bit are permitted; MPPE 40 bit or MPPE 128 bit are permitted; or MPPE 128 bit is permitted, in Encryption.
3. When setup is complete, click [Save].
4. When [Restart] is displayed on the setup page, click it.

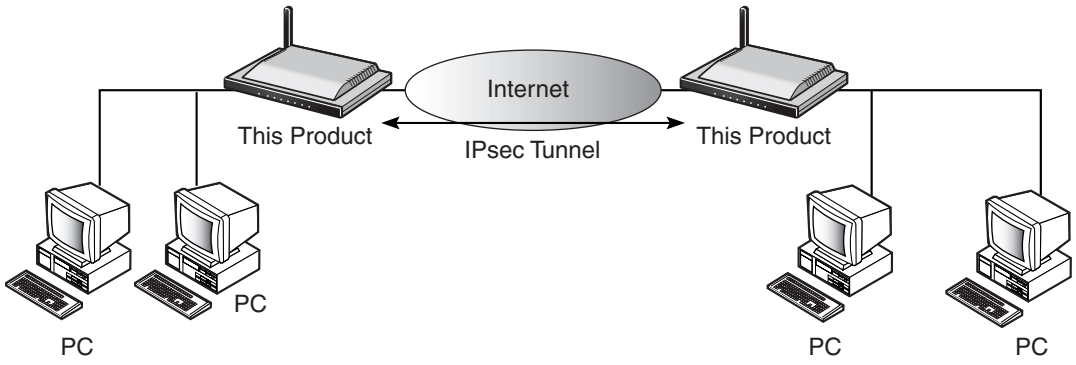

Authentication
Select the encryption method of the password.
MS-CHAP or MS-CHAPv2 are used.
Only MS-CHAPv2 is used.
Encryption
Select the encryption method of the body of the message.
None, MPPE 40 bit, or MPPE 128 bit are permitted
MPPE 40 bit or MPPE 128 bit are permitted
MPPE 128 bit is permitted.
Save
Cancel

Data Entry Field

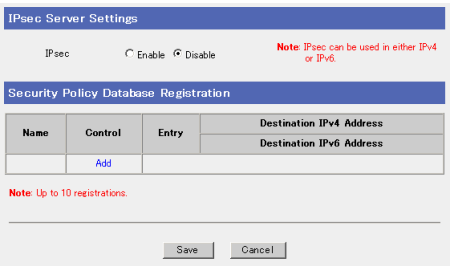
Authentication	This function allows you to specify a password authentication method. When PPP connected, the MS-CHAP and MS-CHAPv2 use an encryption authentication method whereby the user name and password are encrypted and authenticated. The MS-CHAP authenticates encrypted data in one direction, from the client to this product only. Whereas the MS-CHAPv2 authenticates data traveling in both directions, so is even more secure than the MS-CHAP. Select MS-CHAP or MS-CHAPv2 are used; or Only MS-CHAPv2 is used. The default is set to MS-CHAP or MS-CHAPv2 are used.
Encryption	This function allows you to specify an encryption method for the main body of the message. MPPE encrypts VPN connection data using PPTP. There are two encryption methods, which are MPPE 128 bit (strong) and MPPE 40 bit (standard), and data security between this product and the PPTP connection is consolidated. Check either None, MPPE 40 bit or MPPE 128 bit are permitted; MPPE 40 bit or MPPE 128 bit are permitted; or MPPE 128 bit is permitted. The default is set to MPPE 40 bit or MPPE 128 bit are permitted.

3.2.7 Using VPN (IPsec)

This function allows you to construct a VPN using IPsec. A VPN is private network that is as safe as an exclusive line and travels through the Internet. You may need specialist knowledge when performing these settings.



1. Click Add under the Control heading.
- The Destination Information page is displayed.

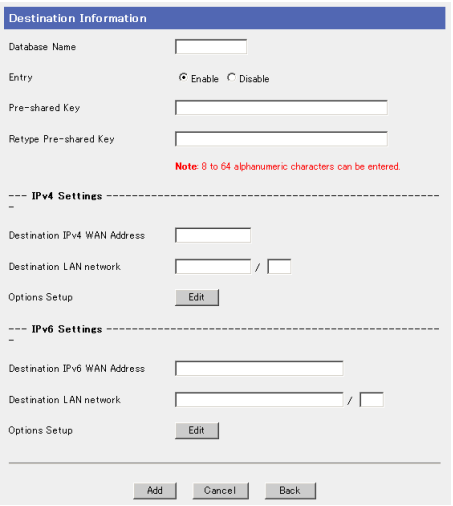


2. Enter the necessary data and click [Add].
- After restart is performed, the top page will be displayed.
- Up to 10 databases can be registered.

3. Check Enable next to IPsec.
- Either the initiator or responder of this product will operate.

4. Click [Save].

5. Click [Restart].



Notes
- After adding a Security Policy Database, ensure that IPsec is set to Enable before saving.

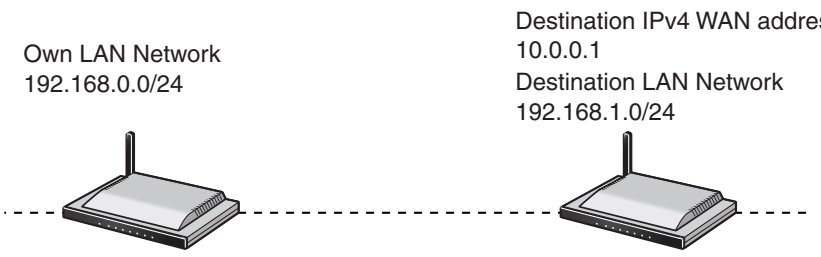
Security Policy Database Registration

Up to 10 security policy database entries can be made.

Data Entry Field

Database Name	Enter a database name up to 10 alphanumeric characters.
Entry	Selecting Enable, enables the entered IPsec settings. When you do not want to use IPsec select Disable. Even if Disable is selected the entered settings will not be deleted.
Pre-shared Key	Sets the pre-shared key. Enter between 8 and 64 alphanumeric characters. The secret shared key used in IPsec is created based on the pre-shared key, so do not let third parties know your pre-shared key. This is in order to maintain communication security.
IPv4 Settings **Destination IPv4 WAN address**	Sets the other party's WAN IPv4 address.
Destination LAN network	Set the destination's LAN network prefix and prefix length. Make sure that this product's LAN side network is a different network from the destination's LAN side network.
Options Setup	Sets detailed IPsec-related settings. (see page 94)
IPv6 Settings **Destination IPv6 WAN address**	Sets the other party's WAN IPv6 global address.
Destination LAN network	Set the other party's LAN network prefix and prefix length. Set a global prefix for the prefix. Also, make sure that this product's LAN side network is a different network from the destination's LAN side network. Please note that a link local address cannot be set.
Options Setup	Sets detailed IPsec-related settings. (see page 96)

IPsec (IPv4) Connection Example

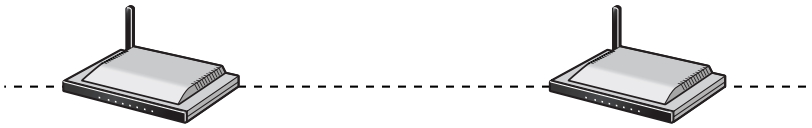


[IPv4 Settings]
Enter "10.0.0.1" for the Destination IPv4 WAN address.
Enter "192.168.1.0", prefix length "24" for the Destination LAN network.

IPsec (IPv6) Connection Example

Own LAN Network
2001:1001: ＊＊＊＊::/64

Destination IPv6 WAN address
2001:1002::＊＊＊＊
Destination LAN Network
2001:1002: ＊＊＊＊::/64



[IPv6 Settings]
Enter "2001:1002:: ＊＊＊＊" for the Destination IPv6 WAN address.
Enter "2001:1002: ＊＊＊＊", prefix length "64" for the Destination LAN network.

IPsec (IPv4)/IPsec (IPv6) Connection Example

Own LAN Network
192.168.0.0/24

Destination IPv4 WAN address
10.0.0.3
Destination LAN Network
192.168.3.0/24

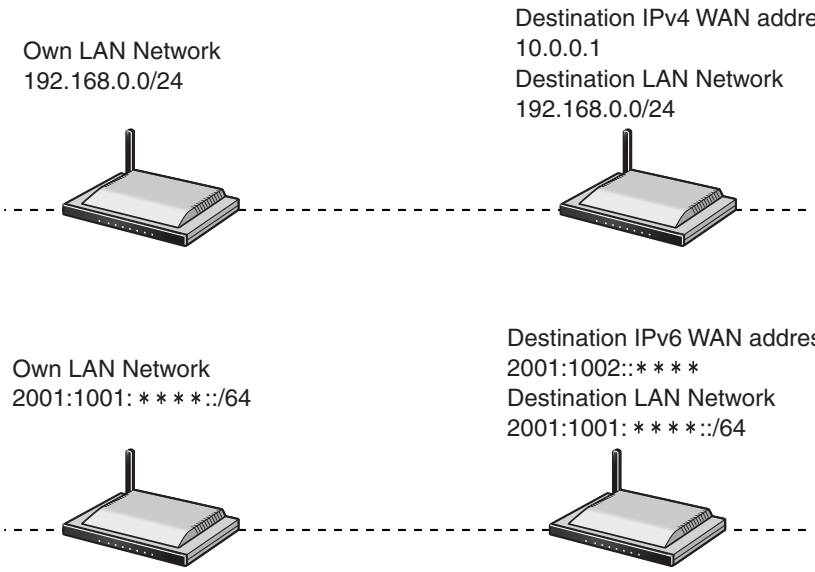
Own LAN Network
2001:1001: ＊＊＊＊::/64

Destination IPv6 WAN address
2001:1004::＊＊＊＊
Destination LAN Network
2001:1004: ＊＊＊＊::/64

[IPv4 Settings]
Enter "10.0.0.3" for the Destination IPv4 WAN address.
Enter "192.168.3.0", prefix length "24" for the Destination LAN network.

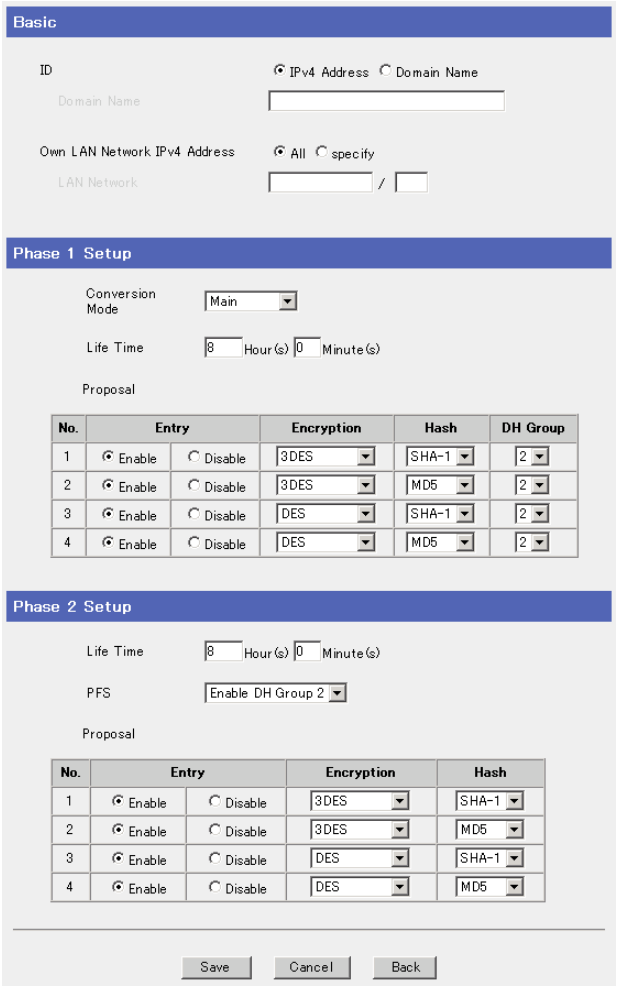
[IPv6 Settings]
Enter "2001:1004:: ＊＊＊＊" for the Destination IPv6 WAN address.
Enter "2001:1004: ＊＊＊＊", prefix length "64" for the Destination LAN network.

Examples of when this products cannot be connected via IPsec
In the example below, IPsec will not operate because the two networks are the same.



IPsec (IPv4) Options Setup

It is possible to perform detailed IPsec (IPv4) connection settings. Usually they do not need to be modified. You may need specialist knowledge when performing these settings.



Basic

ID	Set an ID indicating your identity. You can set an IPv4 Address or Domain Name. If a Domain Name is set, set the Conversion Mode to Aggressive.
Domain Name	When your ID is a Domain Name, set it here.
Own LAN Network IPv4 Address	Set All or Specify the source IP address of the packet. When selecting All, targets the network that is set by this product's LAN side IP address setting, and encapsulates the packet by IPsec. When selecting Specify, targets the address that is specified by LAN Network, and encapsulates by IPsec.
LAN Network	Set the packet source network address of this product's LAN side network when Own LAN Network IPv4 Address is set as Specify.

Phase 1 Setup

Conversion Mode	Set the IKE phase 1 conversion mode to Main or Aggressive. The key conversion procedure for Aggressive is simpler but security is slightly reduced.
Life Time	Set the IKE SA lifetime. The time must be set between 5 minutes and 2400 hours.
Proposal Entry	Set whether to Enable or Disable this proposal. Proposals that are disabled will not be proposed.
Proposal Encryption	Set the method of encryption used in phase 1. Select an encryption method from DES, 3DES, AES (128 bit), AES (192 bit), and AES (256 bit).
Proposal Hash	Set the authentication algorithm (hash). Select from MD5 and SHA-1.
Proposal DH Group	Set the DH (Diffie-Hellman) group used in phase 1. Select between 1 and 2. DH group 2 is has increased security compared to DH group 1, but group 1 is not weak. When the conversion mode is set to Aggressive, both IPsec devices must have the same DH group set.

Phase 2 Setup

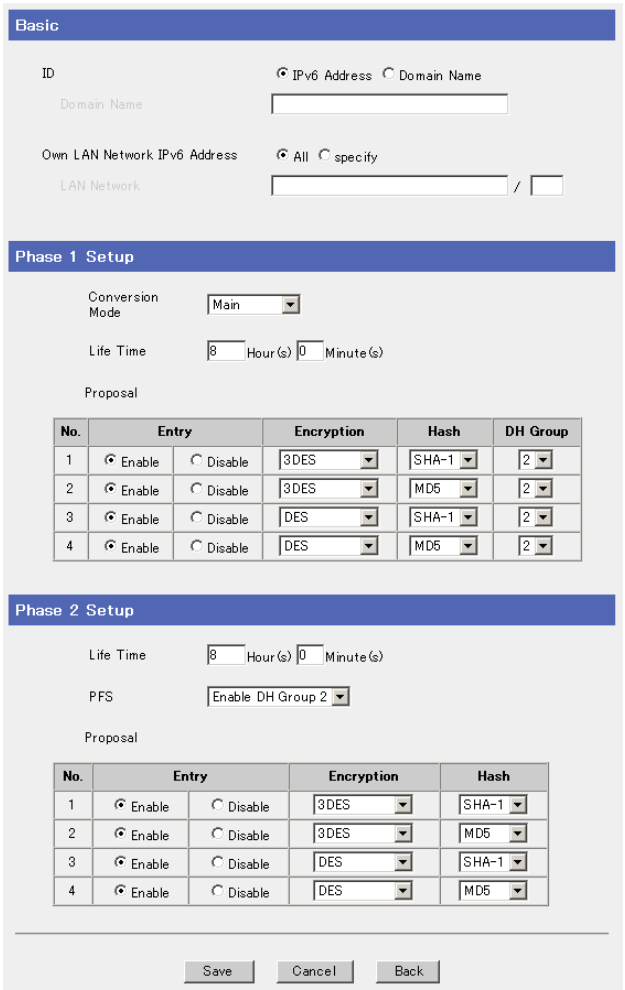
Life Time	Set the IPsec SA lifetime. The time must be set between 5 minutes and 2400 hours.
PFS	Set whether to enable PFS (Perfect Forward Security) in phase 2. Select from Enable DH Group 2, Enable DH Group 1, and Disable. When Enable Group 2 is selected, the Diffie-Hellman exchange is re-performed in phase 2, and DH Group 2 creates a secret shared key. When Enable Group 1 is selected, the Diffie-Hellman exchange is re-performed in phase 2, and DH Group 1 creates a secret shared key. When Disabled is selected, the secret shared key created in phase 1 is used in phase 2. Security is increased when PFS is enabled rather than disabled.
Proposal Entry	Set whether to Enable or Disable this proposal. Proposals that have Disable set will not be proposed.
Proposal Encryption	Set the method of encryption. Select an encryption method from DES, 3DES, AES (128 bit), AES (192 bit), AES (256 bit) and NULL.
Proposal Hash	Set the authentication algorithm (hash). Select from MD5, SHA-1, and None (authentication algorithm not used).

Note

You cannot select NULL for Encryption and None for Hash simultaneously in phase 2.

IPsec (IPv6) Options Setup

It is possible to perform detailed IPsec connection settings. Usually they do not need to be modified. You may need specialist knowledge when performing these settings.



Basic

ID	Set an ID indicating your identity. You can set an IPv6 Address or Domain Name. If a Domain Name is set, set the Conversion Mode to Aggressive.
Domain Name	When your ID is a Domain Name, set it here.
Own LAN Network IPv6 Address	Select All or Specify packet source IP addresses. When All is selected, the packets of all global addresses on the LAN side, are encapsulated using IPsec. When selecting Specify, targets the global address that is specified by LAN Network, and encapsulates by IPsec.
LAN Network	Set the packet source network address (prefix) of this product's LAN side network when Own LAN Network IPv6 Address is set as Specify.

Phase 1 Setup
See page 95 to set up phase 1.

Phase 2 Setup
See page 95 to set up phase 2.

3.2.8 Using Applications

This product, apart from the basic programs (firmware) that control the camera, has an application platform function.

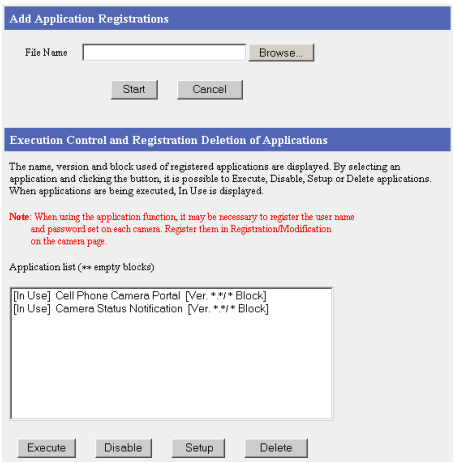
* The Panasonic Support Website is located at **http://panasonic.co.jp/pcc/products/en/netwkcam/**.

Note

This product comes with the Camera Status Notification and Cell Phone Camera Portal applications pre-installed.

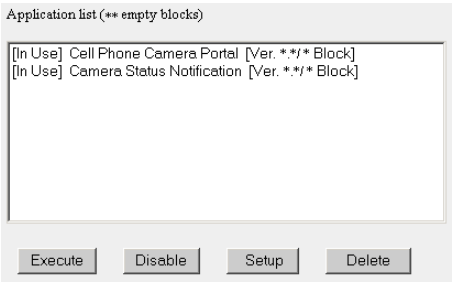
Registering Applications

1. Click [Applications] on the setup page.
2. To choose an application, click [Browse...].
   - The Choose File dialog box is displayed.
3. Select the application you want to install from the file list, and click [Open].
   - The selected file is displayed in the File Name field.


Add Application Registrations
File Name
Browse...
Start
Cancel
Execution Control and Registration Deletion of Applications
The name, version and block used of registered applications are displayed. By selecting an application and clicking the button, it is possible to Execute, Disable, Setup or Delete applications. When applications are being executed, In Use is displayed.
Note: When using the application function, it may be necessary to register the user name and password set on each camera. Register them in Registration/Modification on the camera page.
Application list (** empty blocks)
[In Use] Cell Phone Camera Portal [Ver. *.*/* Block]
[In Use] Camera Status Notification [Ver. *.*/* Block]
Execute
Disable
Setup
Delete

4. Click [Start].

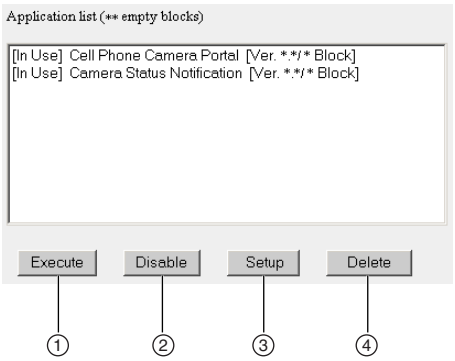
After an application has been registered, it is displayed on the Application list.



Note

These applications are only available when using IPv4 and not IPv6. Also, they are not available when using IPv6-supported cameras.

Application List



① Executes disabled applications. (see below)

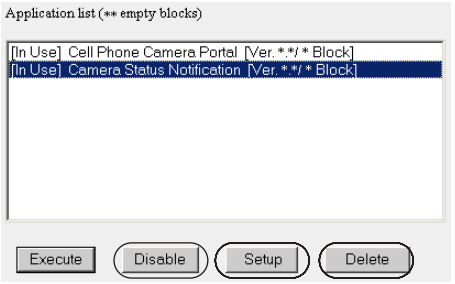
② Disables applications. (see below)

③ It may be necessary to change settings depending on the application. (see the Instructions for each application)

④ Deletes applications. (see below)

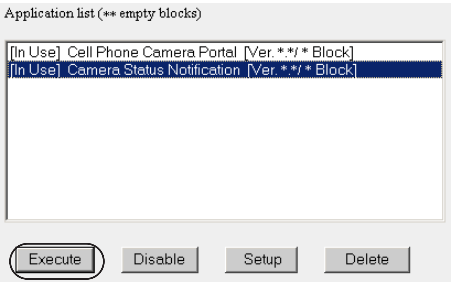
Controlling and Deleting Applications

1. Click [Applications] on the setup page.
2. Select an application and click either [Disable], [Setup] or [Delete].
   - When deleting, a confirmation dialog box is displayed. Check whether the application is correct and click [Yes].
   - See the Instructions of each application for more information on the Setup page.


Application list (** empty blocks)
[In Use] Cell Phone Camera Portal [Ver. *.*/ * Block]
[In Use] Camera Status Notification [Ver. *.*/ * Block]
Execute
Disable
Setup
Delete

Executing Disabled Applications

1. Click [Applications] on the setup page.
2. Select an application and click [Execute].


Application list (** empty blocks)
[In Use] Cell Phone Camera Portal [Ver. *.*/ * Block]
[In Use] Camera Status Notification [Ver. *.*/ * Block]
Execute
Disable
Setup
Delete

Notes

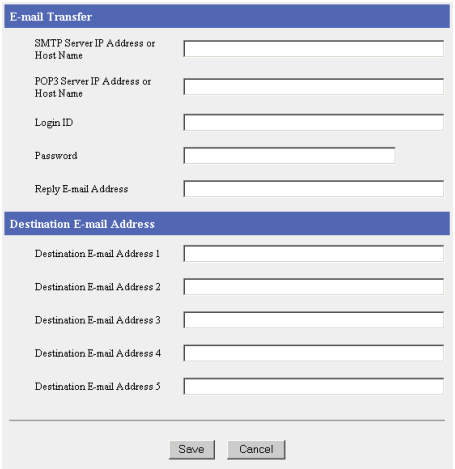
- **In default settings the applications are disabled. To start an application click [Execute].**
- When this product is restarted, applications will remain in the current status (executed or disabled).

Application E-mail

This function allows you to set mail forwarding used in the application platform function.

- This setting may be necessary depending on the application.

1. Click [E-mail Setup for Applications].
2. Set each heading and click [Save].
3. Click [Restart].



Data Entry Field

SMTP Server IP Address or Host Name	Enter the sent mail (SMTP) server's address*1 or host name (1-255 characters)*2.
POP3 Server IP Address or Host Name	Enter the received mail (POP3) server's address*1 or host name (1-255 characters)*2.
Login ID	Enter the received mail (POP3) server's login ID.*3
Password	Enter the received mail (POP3) server's password.*3
Reply E-mail Address*2	Enter the return destination's (sent source) E-mail address. It is recommended that you enter the administrator's E-mail Address.
Destination E-mail Address 1 - Destination E-mail Address 5*2	Up to 5 E-mail destinations can be set.

*1 Set 4 numbers (0-255) and 3 periods, in the form of 192.163.0.253 (However 0.0.0.0 or 255.255.255.255 cannot be used.)

*2 Only alphanumeric characters can be used. However, [Space], ["], ['], [#], [&], [%], [=], [+], [?], [<], [>], and [:] cannot be used.

*3 When POP3 authentication is required during mail forwarding, set it, checking with the network administrator or ISP.

Note

SMTP authentication is not supported.

3.3 Managing This Product

3.3.1 Changing The Password

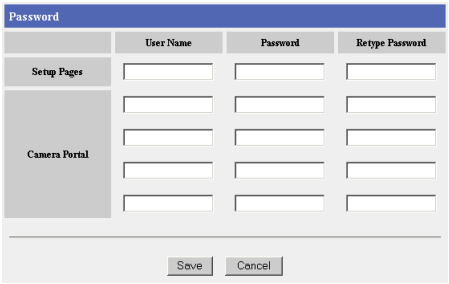
This function allows you to change the password for access to the Camera Portal and the setup page.

1. Click [Password] on the setup page.

2. Enter a new User Name (6 - 15 characters) in the User Name data field in either the Setup Pages or Camera Portal.

3. Enter a new Password (6 - 15 characters) in the Password data field, then re-enter in the Retype Password data field.

- You can set one password in Setup Pages and up to 4 in Camera Portal.



Notes

- When re-entering the password, do not use the copy or paste functions.
- User names and passwords are case-sensitive.

4. Click [Save].

- When password modification is complete, the window on the right will be displayed.

New settings are saved.
It is necessary to restart this product to complete the setting.
If you want to restart later, click the restart button on the restart page.
If you want to restart it immediately, click the restart button below.
Restart

- If the entered password is incorrect, the window on the right will be displayed.

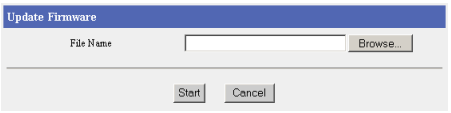
If you forget your user name and password...
Push the FACTORY DEFAULT RESET button and initialize this product. (see page 117)
Settings will return to the default state. Re-set the user name and password.

3.3.2 Updating Firmware

To prevent leaks of customer information, illegal operation of this product, interference or involuntary shutdown etc, update firmware regularly. The most recent firmware file can be found on Panasonic's Support Website (**http://panasonic.co.jp/pcc/products/en/netwkcam/**).

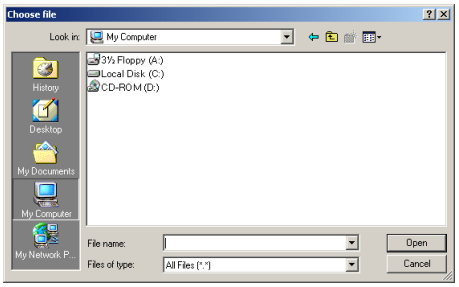
Before using the update firmware function, download the firmware file to your PC. See the support website for more details.
When downloading an old firmware version, the setup information may be reset to factory default. See Release Note for more details.

1. Click [Update Firmware] on the setup page.



2. Click [Browse...] to select the firmware file.
- The Choose file window is displayed.

3. Select the firmware file you want to install from the file list, and click [Open].
- The selected file is displayed in the File Name field of the update firmware page.



4. Click [Start].
- Firmware is updated.

Note

When updating firmware do not cut the power supply. If cut, the update might not be completed successfully.

(If the power is inadvertently cut, the power indicator will blink green the next time power is turned on. Re-update firmware referring to The POWER indicator is blinking green (see page 31) in Installation/Troubleshooting).

- When the firmware update is complete, this product will automatically restart.
- If the firmware update was not completed successfully, an error message will be displayed. (see table below)

Notes

- It may be necessary to initialize settings after updating firmware. See Panasonic's Support Website for details. Push the FACTORY DEFAULT RESET button to re-initialize. (see page 117)
- When using the DHCP server function (see page 77), restart all the LAN (Home) side PCs connected to this product.

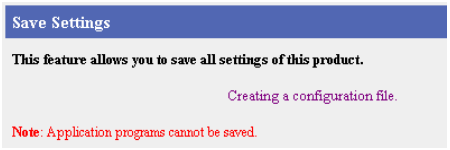
Error Message	Cause and Remedy
Incorrect file	The firmware file you have selected is invalid for this product. Select a valid file. See the explanation (readme.txt etc.) attached to the file, and check that it is compatible with this product's software version. (see page 109) When it is not compatible, download a more recent firmware file, which is compatible with the software version from **http://panasonic.co.jp/pcc/products/en/netwkcam/**.

Error Message	Cause and Remedy
Out of Memory	The built-in memory of this product is reduced due to load processing. After restarting this product, re-update the firmware.

3.3.3 Saving Settings

This function allows you to save setup files, and load the saved files.

Save Settings

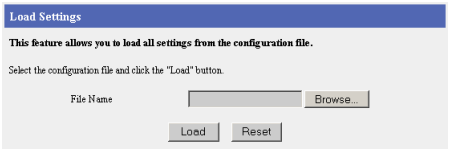

Save Settings
This feature allows you to save all settings of this product.
Creating a configuration file.
Note: Application programs cannot be saved.

1. Click [Save Settings] on the setup page.
2. Click Creating a configuration file.
   - The download wizard window is displayed.
3. Specify the Location and File name, and Save.

Note

Applications cannot be saved.

Load Settings


Load Settings
This feature allows you to load all settings from the configuration file.
Select the configuration file and click the "Load" button.
File Name
Browse...
Load
Reset

1. Click [Save Settings] on the setup page.
2. Click [Browse...] to select the file to be loaded.
   - The Choose File window is displayed.
3. Select the file to be loaded from the file list, and click [Open].
   - The selected file is displayed in the File Name field of the loading settings page.
4. Click [Load].
5. Click [Reboot].
   - This product is restarted.

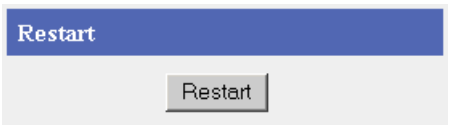
Notes

- When the file you are attempting to load is damaged or invalid, an error message is displayed.
- After loading settings, all applications are disabled. Execute the application function on the setup page.

3.3.4 Restarting

When restarting, this product's setup information is saved.

1. Click [Restart] on the setup page.



2. Click [Restart].
   - This product is restarted.

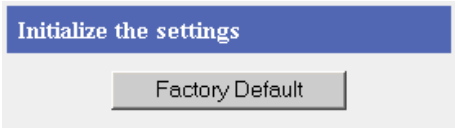
Notes

- When using the DHCP server function (see page 77), restart all LAN (Home) side PCs connected to this product.
- When this product is restarted, applications will remain in the current status (executed or disabled).

3.3.5 Initializing The Settings

This function resets all settings to the factory default. (see page 140)

1. Click [Factory Default] on the setup page.



2. Click [Factory Default].
   - All settings are reset.

Notes

- When using the DHCP server function (see page 77), restart all LAN (Home) side PCs connected to this product.
- Applications cannot be reset to factory default. When resetting factory default, all applications are disabled. Execute the application function on the setup page.

3.3.6 Using PPPoE Connection

This function allows you to manually connect/disconnect the PPPoE connection to your ISP. When cutting this product's power supply, manually disconnect the PPPoE connection before doing so. If the power is turned off before PPPoE is manually disconnected, it may take some time to re-connect once the power has been turned back on.

Connecting PPPoE

1. Click [PPPoE Connection] on the setup page.
2. Click [Connect] to start PPPoE connection.

Disconnecting PPPoE

1. Click [PPPoE Connection] on the setup page.
2. Click [Disconnect] to disconnect.

Notes

- This function can be used irrespective of the type (always or manual) of PPPoE connection.
- If PPPoE is disconnected from the WAN (Internet) side, this product cannot be re-accessed from the WAN side.

Session keep-alive function

This product has a session keep-alive function. This is when using the always mode of PPPoE connection, if connection with the ISP's server is disconnected for some reason, the session keep-alive function automatically tries to regain connection. This function also has the following characteristics:

- It is enabled during always connection mode. During manual connection mode, it will not connect automatically.
- It will try to regain connection after 1, 2, 3....9, 10 minutes, and every 10 minutes after that.

3.3.7 Using VPN (IPsec) Connection

This function allows you to manually connect and disconnect VPN (IPsec) connection.

Connecting VPN (IPsec)

1. Click [VPN (IPsec)] on the setup page.
2. Click [Connect] to start VPN (IPsec) connection.

Disconnecting VPN (IPsec)

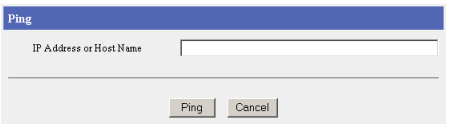
1. Click [VPN (IPsec)] on the setup page.
2. Click [Disconnect] to disconnect.

3.3.8 Confirming Network Connection

The Ping function allows you to check if each device on the WAN (Internet) side or LAN (Home) side is connected to this product on a TCP/IP network. When a device is connected successfully, Success! is displayed.

1. Click [Ping] on the setup page.

2. Enter the IP address (e.g. "**192.168.0.1**") or host name of the device you would like to check.
   - Click [Cancel] to return the IP address or host name fields to a blank field.



3. Click [Ping].
   - When a device is connected successfully, the window on the right is displayed.

   - When there is no response from the specified IP address, the window on the right is displayed.

Notes

- Even if the website can be accessed, sometimes it cannot respond to the Ping.
- When the host name cannot be found in the DNS, "XXX is not found" is displayed.
- An IPv6 address cannot be entered.

3.4 Getting Information

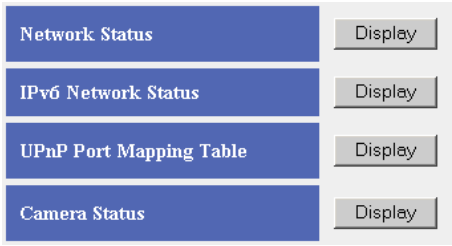
3.4.1 Getting Network Information

This page displays information that is useful when contacting an authorized servicenter, such as Network Status, UPnP Port Mapping Table and Camera Status.

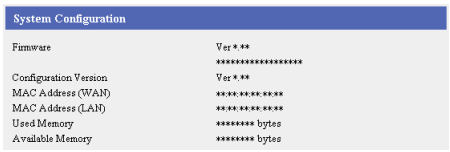
Network Status and IPv6 Network Status

These pages show hardware and software version information for IPv4 and IPv6 connections. This information is useful when contacting an authorized servicenter.

1. Click [Status] on the setup page.
   - When displaying IPv6 Network Status, click IPv6 Setup on the menu page before clicking Status.



2. Click [Display] Network Status.
   - Click [Display] IPv6 Network Status for IPv6 network information.



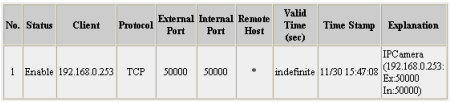
Note

When [Save] at the bottom of the page is clicked, the file download window is displayed. Specify the Location and File Name, and save the contents displayed.

UPnP™ Port Mapping Table

UPnP™ port mapping information registered on this product is displayed. Up to 128 pieces of information can be displayed. When restarting this product, UPnP™ port mapping registration information is deleted.
UPnP™ port mapping information can be checked by following the steps below:

1. Click [Status] on the setup page.
2. Click [Display] UPnP Port Mapping Table.



No.	Status	Client	Protocol	External Port	Internal Port	Remote Host	Valid Time (sec)	Time Stamp	Explanation
1	Enable	192.168.0.253	TCP	50000	50000	*	indefinite	11/30 15:47:08	IPCamera (192.168.0.253: Ex:50000 In:50000)

Headings Displayed

Registered UPnP™ port mapping information

No.	The maximum number of UPnP™ port mapping registrations is 128. Two types of status are shown below: 1 When IGD in UPnP in Options is set to Enable, No. of Current Registrations/128 is displayed in the No. column. 2 When IGD in UPnP in Options is set to Disable, 0/128 is displayed in the No. column.

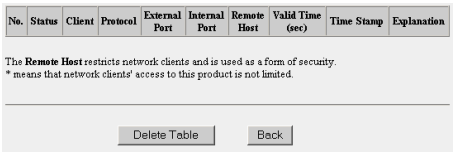
Status	Displays whether port mapping is enabled or disabled.
Client	The client's IP address is displayed.
Protocol	The protocol, which is subject of the set information, is displayed. Either TCP or UDP is displayed.
External Port	The external (WAN side) port number in the set port information is displayed.
Internal Port	The client side's port number in the set port information is displayed.
Remote Host	When the client requests additional ports from a specified network device, the device's host IP address is displayed. If there is no access control, " * " is displayed.
Valid Time (sec)	When an valid time is set for the registered UPnP™ port by the client, that valid time is displayed in seconds. When an valid time is not set, indefinite is displayed.
Time Stamp	The time when the client first registered using UPnP™ is displayed. The time is calculated based on the PC's clock. If the time looks incorrect, adjust your clock's settings.
Explanation	Information sent from applications is displayed.

Deleting UPnP™ port mapping registered information

This function allows you to delete the UPnP™ port mapping table registered on this product. The whole of the table will be deleted by clicking the delete table button.

Take the following steps to delete the registered UPnP™ port mapping table:

1. Click [Delete Table] on the UPnP port mapping table page.
   - A window indicating that the table has been deleted is displayed.



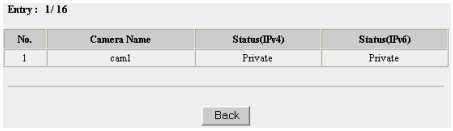
Notes

- Even if Windows/MSN Messenger is shutdown, UPnP™ port mapping can sometimes remain. Therefore, when the number of UPnP™ port mapping registrations exceeds the maximum of 128, those new registrations are ignored and Windows/MSN Messenger cannot be used. In that case, delete the port mapping table once.
- When the registered UPnP™ port mapping information is deleted and the connection is cut while Windows/MSN Messenger is activated, shut Windows/MSN Messenger down once and restart it again. Windows/MSN Messenger will not work by simply signing in again.

Camera Status

This function displays the registered information of cameras connected to this product. The maximum number of cameras is 16. These are cameras that have been setup automatically. The information for cameras setup manually is not displayed. Take the following steps to check the camera information.

1. Click [Status] on the setup page.
2. Click [Display] Camera Status.



3.4.2 Viewing Logs

This function displays the various logs created by this product. The logs are displayed from the most recent first, and when full, they are deleted and replaced by new logs.

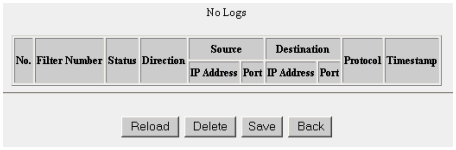
Notes

- It is important to always use your user name and password for authentication when using this product.
- Access information (user name/password), this product's setup information, application setup information, logs and other system management information is the responsibility of the customer. Access to this information should be limited to users or user groups, and third parties should not be allowed to refer to, modify, delete or copy this information. Information such as user name, password, setup and management information should be kept confidential.
- The log time is calculated based on the clock of the PC that monitors the log. If the time looks incorrect, adjust your clock's settings and re-display the log.
- When restarting, log information is deleted.
- By clicking [Save] at the bottom of each display page, the file download window is displayed. Specify the Location and File Name, and Save the contents displayed.

Filtering Log and IPv6 Filtering Log

This function allows packet information to be registered, if the packet is processed by the entry checked in [Log Output] on the packet filtering page. Packet information such as filter number, status, direction, and source/destination port number, up to 4000 pieces of information can be viewed. When connecting using IPv6, it is possible to view IPv6 filtering logs.

1. Click [Log] on the setup page.
2. Click [Display] Filtering Log.
3. Click [Reload] to display the latest log page.
   - To delete a recorded log, click [Delete].



Note

When the filter number of the log is displayed as "P-P", "SHR", "W-C", "W-P", "STL", "STL (Ident)", "SPI", "DoS", or "GOR", easy security settings filtering is being displayed. See pages 67 and 72 for more details.

UPnP™ Log (General) and UPnP™ Log (CP)

The UPnP™ logs (general) function allows you to display a list of logs of port mapping additions, deletions, and failures. The UPnP™ logs (CP function) function allows you to display a list of logs of UPnP™ CP function port mapping additions, deletions, and failures. The maximum number of saved logs and the maximum number of logs on one page is 400.

1. Click [Log] on the setup page.
2. Click [Display] UPnP Log.
3. Click [Reload] to display the latest log page.
   - To delete a recorded log, click [Delete].

Headings Displayed

No.	This is the log number. Numbers are attributed from the most recent.
Timestamp	The time when this product performed the port operation is displayed. The time is calculated based on the PC's clock. If the time looks incorrect, adjust your clock's settings.
Event	The content of the port operation is displayed. The message displayed is one of the following: • [Port addition]: Port was added. • [Port addition failure]: Port was not added. • [Port removal]: Port was deleted. • [Port removal (by user operation)]: Port was deleted by the user. • [Port removal failure]: Port was not deleted. • [All port removal (by user operation)]: All ports were deleted by the user. • [Auto port removal (by user operation)]: The time set in Automatic deletion of UPnP port mapping has passed. • [Auto port removal (by application setting)]: The time specified by the application in use has passed. • [Port addition failure (only permanent)]: Port was not added. • [Port addition failure (require same port for internal/external)]: Port was not added.
Client (IP Address, Port)	The client side's IP address and port number in the specified port information is displayed.
Protocol	The protocol for the specified information is displayed. TCP or UDP is displayed.
External Port	The external (WAN side) port number in the specified port information is displayed.

Connection Log

The connection, disconnection and authentication logs during PPPoE or DHCP connection are displayed. You can check the connecting IP address in the connection log. 100 logs can be displayed on 1 page and 400 can be recorded in total. When there are more than 100 logs, select the page number at the bottom of the page and search for the required log.

1. Click [Log] on the setup page.
2. Click [Display] Connection Log.

DynamicDNS Log

This function allows you to display data communication logs to/from the DynamicDNS server. 100 logs can be displayed on 1 page and 400 can be recorded in total.

1. Click [Log] on the setup page.
2. Click [Display] DynamicDNS Log.

VPN (PPTP) Connection Log

This function allows you to register up to 400 VPN (PPTP) Logs. 100 logs can be displayed on 1 page and 400 can be recorded in total.

1. Click [Log] on the setup page.
2. Click [Display] VPN (PPTP) Connection Log.

Mail Transmission Log

This function allows you to view the history of mail transmission. 100 logs can be displayed on 1 page and 400 can be recorded in total.

1. Click [Log] on the setup page.
2. Click [Display] Mail Transmission Log.

VPN (IPv4 IPsec) Connection Log

This function allows you to view the VPN (IPv4 IPsec) logs. 100 logs can be displayed on 1 page and 400 can be recorded in total.

1. Click [Log] on the setup page.
2. Click [Display] VPN (IPv4 IPsec) Connection Log.

VPN (IPv6 IPsec) Connection Log

This function allows you to view the VPN (IPv6 IPsec) logs. 100 logs can be displayed on 1 page and 400 can be recorded in total.

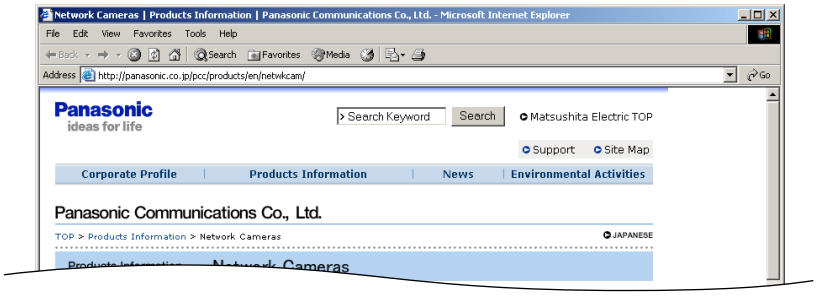
1. Click [Log] on the setup page.
2. Click [Display] VPN (IPv6 IPsec) Connection Log.

3.4.3 Support

The support function allows you to get product and support information from the Internet.

1. Click [Support] on the menu page.
2. Click the URL for product information or support information.
   - The website is displayed.

Example of support information website



3.4.4 Help

The help function explains each heading on the setup page.

1. Click [Help] on the setup page.
2. Select the heading you want to research.

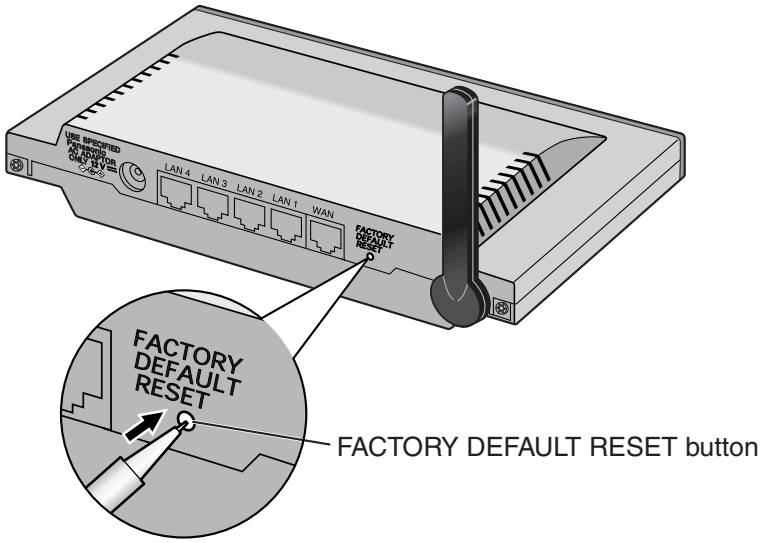
Note

You can also view help by clicking on each heading on that setup page.

4 Other Information

4.1 Factory Default

There is a FACTORY DEFAULT RESET button on the rear of this product. Push this button to initialize the settings.



4.1.1 Factory Default

If you have forgotten your password or want to return the settings to factory default (see page 140), push the FACTORY DEFAULT RESET button for 1 second.

Notes

- Pushing the FACTORY DEFAULT RESET button will delete the current settings and return them to the default settings.
- When using the DHCP server function (see page 77), restart all LAN (Home) side PCs connected to this product.
- Initializing using the FACTORY DEFAULT RESET button and Factory Default on the menu page perform the same operation.
- Applications cannot be initialized. When initializing this product, all applications are disabled. Execute the application function on the setup page.

4.1.2 Restart

When the power indicator is blinking red (see Installation/Troubleshooting on page 30), restart this product. Removing the AC plug from the outlet and re-inserting it, allows you to restart this product without any effect on the settings.

Notes

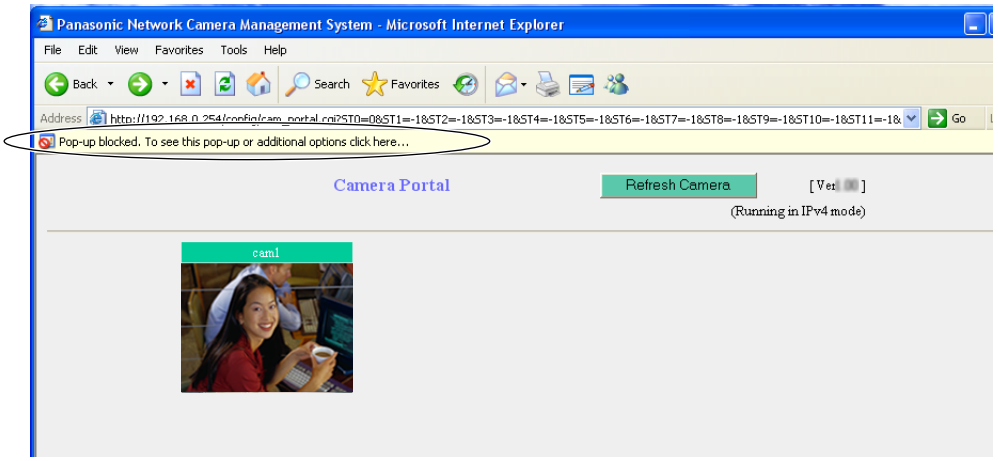
- When using the DHCP server function (see page 77), restart all LAN (Home) side PCs connected to this product.
- When this product is restarted, applications will remain in the current status (executed or disabled).

4.2 Disabling Pop-up Blocker

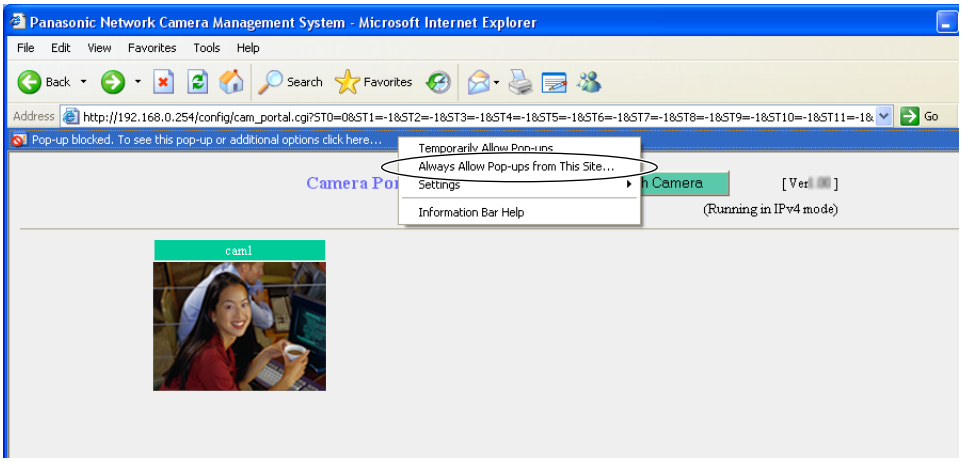
When Microsoft Windows XP Service Pack 2 is used, a pop-up blocker may prevent the camera from displaying the image. The following steps will display the image.

- **Registering the image as the permitted website**

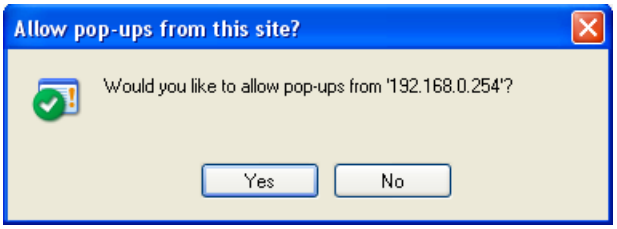
1. Click the warning displayed above the page, and click it.


Panasonic Network Camera Management System - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address
Pop-up blocked. To see this pop-up or additional options click here...
Camera Portal
Refresh Camera
(Running in IPv4 mode)
cam1

2. Click [Always Allow Pop-ups from This Site...].


Panasonic Network Camera Management System - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address
Pop-up blocked. To see this pop-up or additional options click here...
Temporarily Allow Pop-ups
Always Allow Pop-ups from This Site...
Settings
Information Bar Help
(Running in IPv4 mode)
cam1

3. When prompted, click [Yes].



4.3 UPnP™ Setup on your PC

This product allows you to use applications and devices that support UPnP™. The UPnP™ function can be used from either a wire-connected PC or wirelessly connected PC.

UPnP™

Conforming to UPnP™ Forum IGD (Internet Gateway Device), UPnP™ is compatible with the NAT traversal function*. Therefore, Windows/MSN Messenger can be used simultaneously on several PCs connected to the LAN side of this product.

* NAT traversal function
This is a series of functions that, after a network recognition application detects that it is working under the NAT device, distinguishes external IP addresses and sets port mapping which forwards packets from the outside port to the inside port.

UPnP™ Compatible OSs

OSs that are compatible with the UPnP™ function, are as follows:

- Windows XP
- Windows Me

Note

Windows 2000 and Windows 98SE can use this product's UPnP™ function by using MSN Messenger, however it is not officially compatible with the UPnP™ and therefore cannot be guaranteed.

UPnP™ Compatible Applications

Applications that are compatible with the UPnP™ function are as follows:

- MSN Messenger 6.1, Windows Messenger 4.7 (Windows XP)
  Windows Messenger is included with Windows XP as standard, and MSN Messenger can be downloaded from Microsoft's website. MSN Messenger has functions such as Instant Message, Voice Chat, Webcam, Sending Files and Pictures, Remote Assistant, Application Sharing, Whiteboard and Telephone.
- MSN Messenger 6.1 (other than Windows XP)
  Can be used on Windows 2000 or Windows 98SE/Me. MSN Messenger has functions such as Instant Message, Voice Chat, Sending Files and Pictures, and Telephone.

  Notes

  - It is necessary to have DirectX® 8.1 or later installed on the PC using Windows/MSN Messenger.
  - When using the Telephone function, it is necessary to update Windows Messenger's audio related firmware from Microsoft's website.

Number of PCs that can Use the UPnP™ Function

The number of PCs that can use the UPnP™ function depends on the application in use.

Note

The maximum number of port mappings that can be set in UPnP™ setup is 128.

PC Preparation

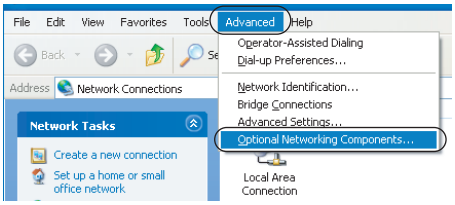
Using Windows XP

- **Windows Messenger:**
  Select Windows Messenger Version Information from the Windows Messenger help menu.
- **MSN Messenger:**
  Download MSN Messenger (Windows XP version) from Microsoft's website and install it. Update your version of MSN Messenger to 6.1.

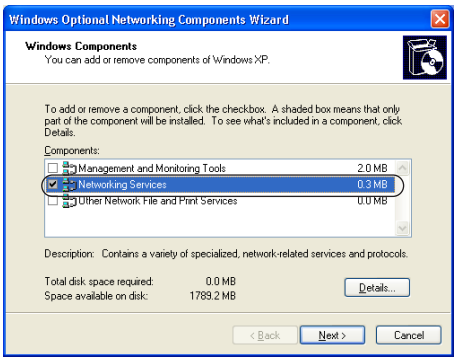
UPnP™ Setup

1. Select My Network Places from My Computer in the Start menu. Then select View network connections.

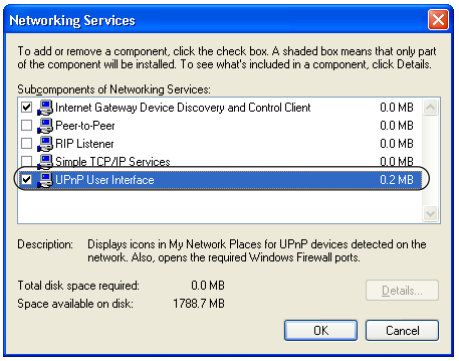
2. Select Optional Networking Components in the Advanced menu.



3. Select Networking Services and click [Details].


Windows Optional Networking Components Wizard
Windows Components
You can add or remove components of Windows XP.
To add or remove a component, click the checkbox. A shaded box means that only part of the component will be installed. To see what's included in a component, click Details.
Components:
Management and Monitoring Tools 2.0 MB
Networking Services 0.3 MB
Other Network File and Print Services 0.0 MB
Description: Contains a variety of specialized, network-related services and protocols.
Total disk space required: 0.0 MB
Space available on disk: 1789.2 MB
Details...
< Back Next > Cancel

4. Check that UPnP User Interface on the Networking Services page is checked.
- If it is not checked, check it and click [OK].
- When the Windows XP CD-ROM is required, follow the instructions displayed.


Networking Services
To add or remove a component, click the check box. A shaded box means that only part of the component will be installed. To see what's included in a component, click Details.
Subcomponents of Networking Services:
Internet Gateway Device Discovery and Control Client 0.0 MB
Peer-to-Peer 0.0 MB
RIP Listener 0.0 MB
Simple TCP/IP Services 0.0 MB
UPnP User Interface 0.2 MB
Description: Displays icons in My Network Places for UPnP devices detected on the network. Also, opens the required Windows Firewall ports.
Total disk space required: 0.0 MB
Space available on disk: 1788.7 MB
Details...
OK Cancel

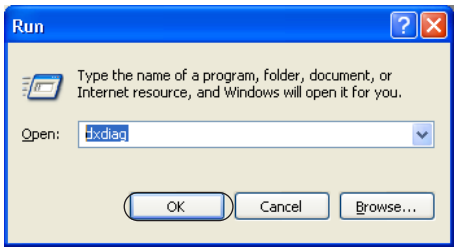
Using Windows 2000, Windows Me or Windows 98SE

Check the Version of MSN Messenger

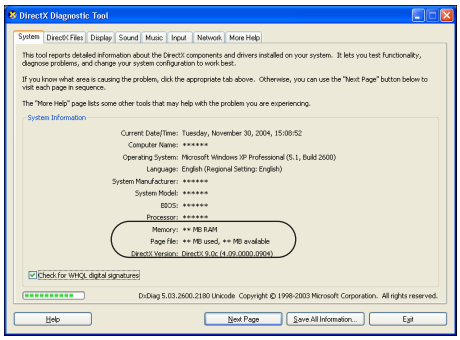
Select [MSN Messenger version information] in the MSN Messenger help menu. Update your version to 6.1.

Check the Version of DirectX

1. Select Run in the Start menu.
2. Enter "**dxdiag**" in the name field and click [OK].



3. Update your version of DirectX if it is older than 8.1.
   - Follow the instructions on the page.



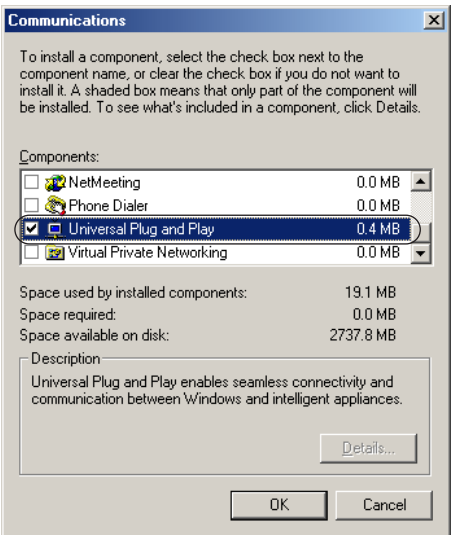
UPnP™ Setup (Windows Me only)

Note

Windows 2000 and Windows 98SE do not have this setting.

1. Select Control Panel from Settings in the Start menu.
2. Double click Add/Remove Program, and then click the Windows Setup tab.

3. Select Communications in Components and click [Details].
   - Check that Universal Plug and Play on the Components page is checked.
   - If it is not checked, check it and click [OK].
   - When the Windows Me CD-ROM is required, follow the instructions on the page.


Communications
To install a component, select the check box next to the component name, or clear the check box if you do not want to install it. A shaded box means that only part of the component will be installed. To see what's included in a component, click Details.
Components:
NetMeeting 0.0 MB
Phone Dialer 0.0 MB
Universal Plug and Play 0.4 MB
Virtual Private Networking 0.0 MB
Space used by installed components: 19.1 MB
Space required: 0.0 MB
Space available on disk: 2737.8 MB
Description
Universal Plug and Play enables seamless connectivity and communication between Windows and intelligent appliances.
Details...
OK
Cancel

Others

Operating Environment

When using Windows/MSN Messenger with UPnP™, restrictions are put on operating environment by the other party.

Note

In environments where, for example, the other party is using a router that is not compatible with UPnP™, or where the private address is connected via an assigned ISP, sometimes data cannot be sent/received when using the Windows/MSN Messenger function.

The layout of the PC screen when connecting this product

Take the following steps when using Windows XP.

1. Connect a PC where UPnP™ is set to ON, to this product.
   - This product's icon is displayed on the PC's My Network Places and Task Tray.
   - The icon is not displayed in Windows 2000 and Windows 98SE.
   - The Task Tray icon is displayed once, and not displayed when connecting for the second time.

2. Double click the My Network Places icon, and find the icon for this product.
   - If necessary, create a shortcut to this product on your desktop.

3. Double click the icon in My Network Places.
- The Enter Network Password window is displayed. By entering the user name and password, this product's setup page is displayed.

Function Name	Windows XP		Windows Me
	Windows Messenger 4.7	MSN Messenger 6.1	MSN Messenger 6.1
Instant Message	Can be used irrespective of settings	Can be used irrespective of settings	Can be used irrespective of settings
Voice Chat	Can be used	Can be used	Can be used
Video Chat	Can be used	Can be used	Function not possible
Sending Files and Pictures	Cannot be used*1	Can be used	Cannot be used*1
Whiteboard	Can be used	Can be used	Function not possible
Application Sharing	Can be used	Can be used	Function not possible
Remote Assistant	Can be used	Can be used	Function not possible
Telephone	Function not possible	Can be used*2	Can be used*2

*1 Due to the connection environment, sometimes data can only be received, and not sent.

*2 There may be cases where data that has been passed previously cannot be received, or phonecalls cannot be made due to the server's status.

Note

For help regarding the functions of Windows/MSN Messenger, see Windows/MSN Messenger help.

4.4 IPv6 Setup on your PC

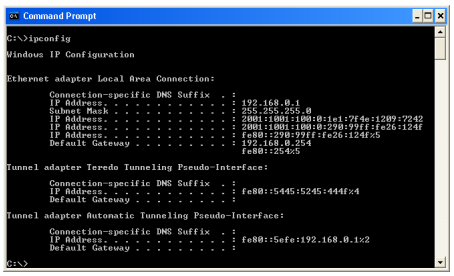
4.4.1 Setting an IPv6 Address Using Windows XP

1. Select [Start] → [All Programs] → [Accessories] → [Command Prompt] and click.
   - The command prompt is started.
2. Enter "ipv6 install", and press [Enter].
   - If Succeeded is displayed, it was installed successfully.

Note

When Windows XP Service Pack 1 is not installed, Succeeded will not be displayed. Install Service Pack 1.

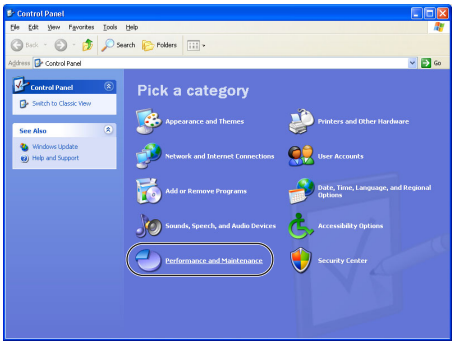
3. Enter "ipconfig" on the command prompt window, and press [Enter].
   - If an IPv6 address is displayed, it has been assigned to this PC.


Command Prompt
C:\>ipconfig
Windows IP Configuration
Ethernet adapter Local Area Connection:
Connection-specific DNS Suffix . :
IP Address. . . . . : 192.168.0.1
Subnet Mask . . . . . : 255.255.255.0
IP Address. . . . . : 2001:1001:100:0:1e1:7f4e:1209:7242
IP Address. . . . . : 2001:1001:100:0:298:99ff:fe26:124f
IP Address. . . . . : fe80:298:99ff:fe26:124f%5
Default Gateway . . . . . : 192.168.0.254
fe80::254%5
Tunnel adapter Teredo Tunneling Pseudo-Interface:
Connection-specific DNS Suffix . :
IP Address. . . . . : fe80::5445:5245:444f%4
Default Gateway . . . . . :
Tunnel adapter Automatic Tunneling Pseudo-Interface:
Connection-specific DNS Suffix . :
IP Address. . . . . : fe80::5efe:192.168.0.1%2
Default Gateway . . . . . :
C:\>

Note

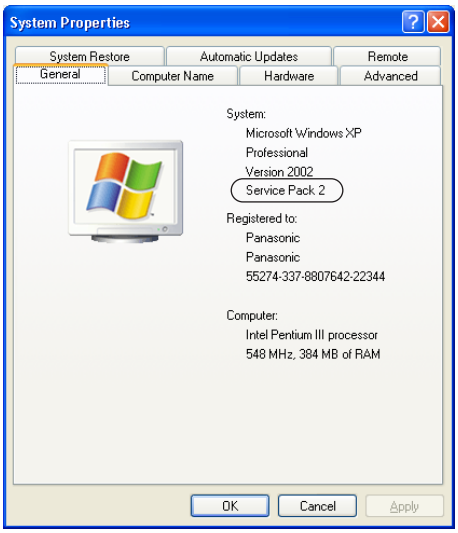
If using Windows XP Service Pack 2, you may not be able to set an IPv6 address. Follow the steps below to check if the PC you are using has Windows XP Service Pack 2 installed.

1. Select [Start] → [Control Panel] and click.
2. Double-click the Performance and Maintenance icon.



3. Double-click the System icon.

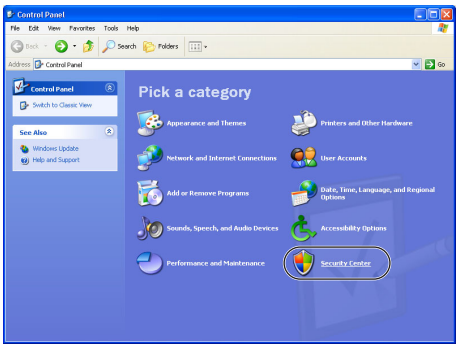
4. Click the General tab, and check if the System is Service Pack 2.



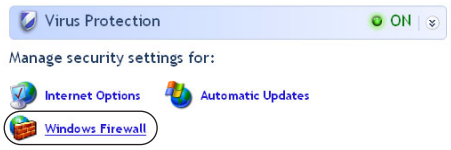
If using Windows XP Service Pack 2, take the following setup steps.

1. Select [Start] → [Control Panel] and click.

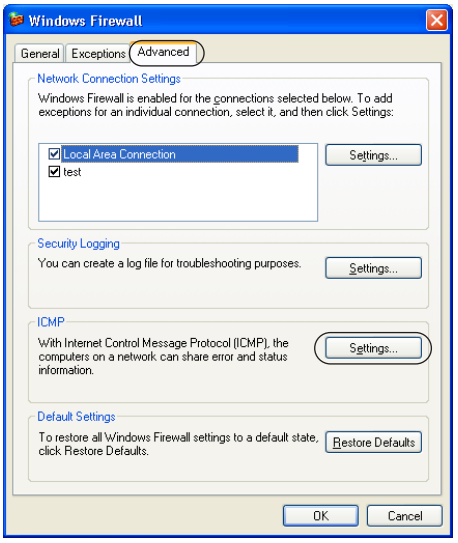
2. Click the Security Center icon.



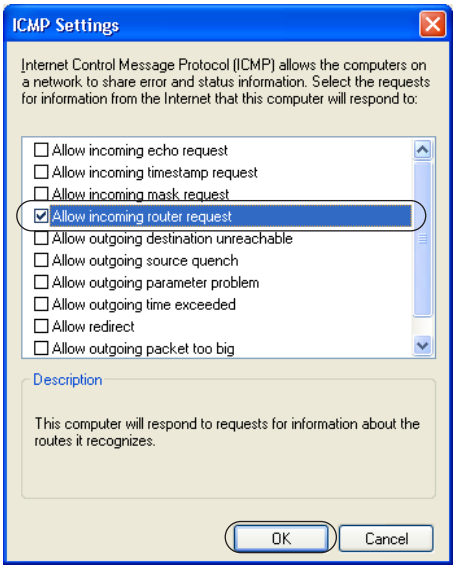
3. Click the Windows Firewall icon.



4. Click the Advanced tab and click [Settings...] for ICMP.


Windows Firewall
General
Exceptions
Advanced
Network Connection Settings
Windows Firewall is enabled for the connections selected below. To add exceptions for an individual connection, select it, and then click Settings:
Local Area Connection
test
Settings...
Security Logging
You can create a log file for troubleshooting purposes.
Settings...
ICMP
With Internet Control Message Protocol (ICMP), the computers on a network can share error and status information.
Settings...
Default Settings
To restore all Windows Firewall settings to a default state, click Restore Defaults.
Restore Defaults
OK
Cancel

5. Check Allow incoming router request on the ICMP Settings window, and click [OK].

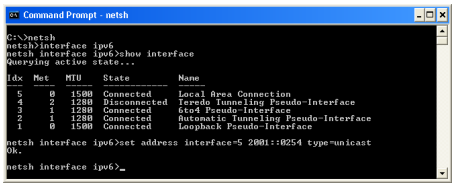

ICMP Settings
Internet Control Message Protocol (ICMP) allows the computers on a network to share error and status information. Select the requests for information from the Internet that this computer will respond to:
Allow incoming echo request
Allow incoming timestamp request
Allow incoming mask request
Allow incoming router request
Allow outgoing destination unreachable
Allow outgoing source quench
Allow outgoing parameter problem
Allow outgoing time exceeded
Allow redirect
Allow outgoing packet too big
Description
This computer will respond to requests for information about the routes it recognizes.
OK
Cancel

4.4.2 Re-obtaining an IPv6 Global Address

1. Select [Start] → [All Programs] → [Accessories] → [Command Prompt] and click.
   - The command prompt is started.
2. Enter "netsh" and press [Enter].
3. On the netsh command line, enter "interface ipv6", and press [Enter].
4. Enter "renew", and re-obtain an IPv6 global address.
5. Enter "exit", press [Enter], and end the netsh command.

4.4.3 Setting a Static IPv6 Global Address.

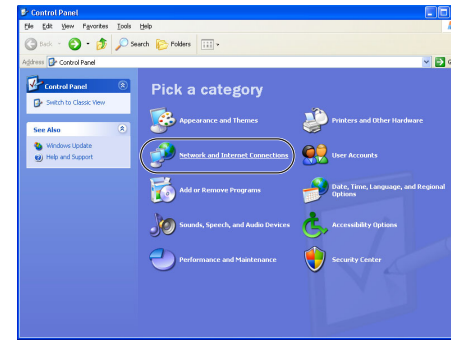
1. Perform steps 1, 2, and 3 in Re-obtaining an IPv6 global address above.
2. Enter "show interface", and press [Enter].
   - Take a note of the Idx number of the Local Area Connection.
3. Next, enter "set address interface=* the IPv6 global address type=unicast", and press [Enter].
   - After "interface=", enter the Idx number noted in step 2.
4. Enter "exit", press [Enter], and end the netsh command.


Command Prompt - netsh
C:\>netsh
netsh>interface ipv6
netsh interface ipv6>show interface
Querying active state...
Idx Met MTU State Name
5 0 1500 Connected Local Area Connection
4 2 1280 Disconnected Teredo Tunneling Pseudo-Interface
3 1 1280 Connected 6to4 Pseudo-Interface
2 1 1280 Connected Automatic Tunneling Pseudo-Interface
1 0 1500 Connected Loopback Pseudo-Interface
netsh interface ipv6>set address interface=5 2001::0254 type=unicast
Ok.
netsh interface ipv6>

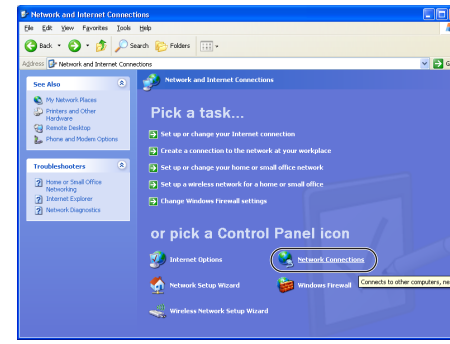
4.5 PPTP Setup when Using VPN: Windows XP

This function sets up a VPN (PPTP) connection on your PC. Take the following steps when using Windows XP.

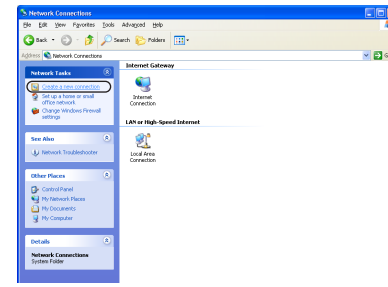
1. Click Network and Internet Connections from Control Panel on the Start menu.



2. Click Network Connections.


Network and Internet Connections
Pick a task...
Set up or change your Internet connection
Create a connection to the network at your workplace
Set up or change your home or small office network
Set up a wireless network for a home or small office
Change Windows Firewall settings
or pick a Control Panel icon
Internet Options
Network Connections
Network Setup Wizard
Windows Firewall
Wireless Network Setup Wizard

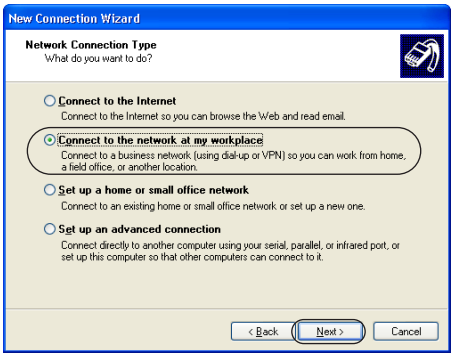
3. Click Create a new connection.



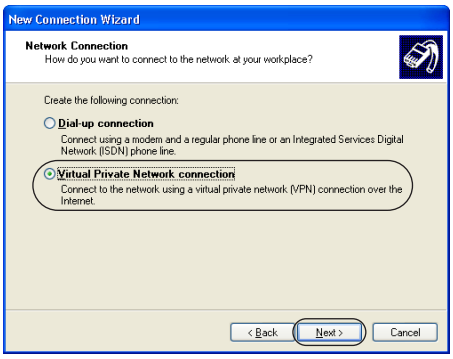
4. Click [Next].

New Connection Wizard
Welcome to the New Connection Wizard
This wizard helps you:
Connect to the Internet.
Connect to a private network, such as your workplace network.
Set up a home or small office network.
To continue, click Next.
< Back
Next >
Cancel

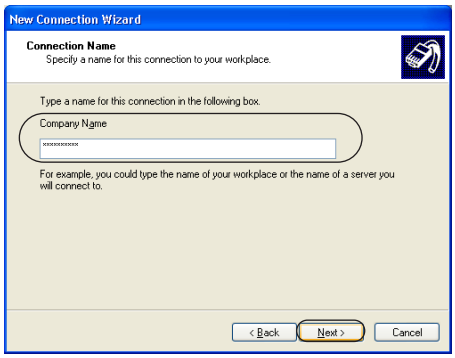
5. Check Connect to the network at my workplace and click [Next].


New Connection Wizard
Network Connection Type
What do you want to do?
Connect to the Internet
Connect to the Internet so you can browse the Web and read email.
Connect to the network at my workplace
Connect to a business network (using dial-up or VPN) so you can work from home, a field office, or another location.
Set up a home or small office network
Connect to an existing home or small office network or set up a new one.
Set up an advanced connection
Connect directly to another computer using your serial, parallel, or infrared port, or set up this computer so that other computers can connect to it.
< Back
Next >
Cancel

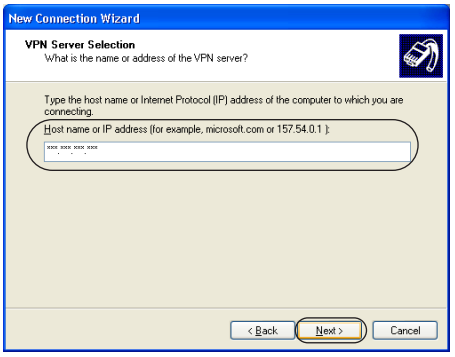
6. Check Virtual Private Network connection and click [Next].


New Connection Wizard
Network Connection
How do you want to connect to the network at your workplace?
Create the following connection:
Dial-up connection
Connect using a modem and a regular phone line or an Integrated Services Digital Network (ISDN) phone line.
Virtual Private Network connection
Connect to the network using a virtual private network (VPN) connection over the Internet.
< Back
Next >
Cancel

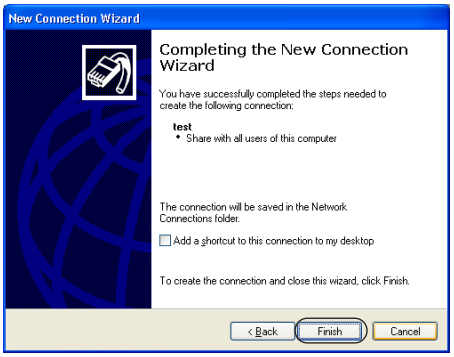
7. Enter the optional network name and click [Next].


New Connection Wizard
Connection Name
Specify a name for this connection to your workplace.
Type a name for this connection in the following box.
Company Name
For example, you could type the name of your workplace or the name of a server you will connect to.
< Back
Next >
Cancel

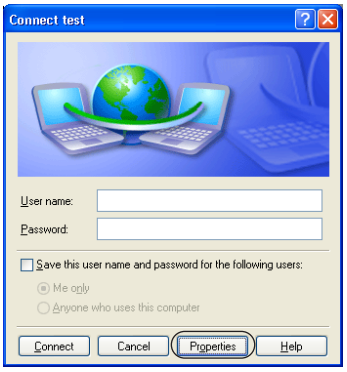
8. Enter this product's WAN IP address and click [Next].


New Connection Wizard
VPN Server Selection
What is the name or address of the VPN server?
Type the host name or Internet Protocol (IP) address of the computer to which you are connecting.
Host name or IP address (for example, microsoft.com or 157.54.0.1):
< Back
Next >
Cancel

9. Click [Finish].

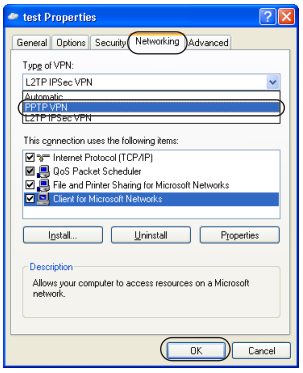

New Connection Wizard
Completing the New Connection Wizard
You have successfully completed the steps needed to create the following connection:
test
• Share with all users of this computer
The connection will be saved in the Network Connections folder.
Add a shortcut to this connection to my desktop
To create the connection and close this wizard, click Finish.
< Back
Finish
Cancel

10. Click [Properties].



11. Click the Networking tab, select PPTP VPN from the VPN dropdown list, and click [OK].

- Set the Security settings and Options settings to match the authentication and encryption methods (see page 89) set on this product.



12. Enter the registered User Name and Password and click [Connect].

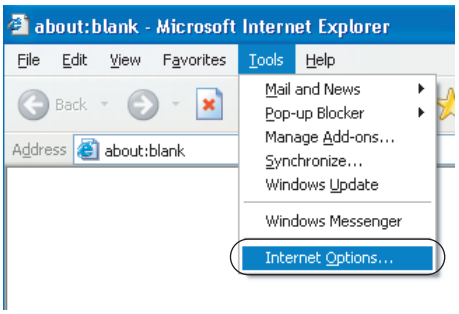
4.6 Web Browser Setup when Using a Proxy Server

The ISP may connect you to the Internet via a proxy server.
When connected via a proxy server, the setup page cannot be accessed. Take the following steps to modify the web browser settings.

The following steps are for when using Internet Explorer 6.0.

1. Start the web browser.

2. Select Internet Options in the Tools menu.



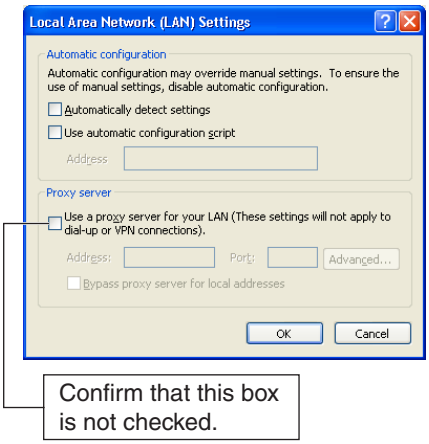
3. Click the Connections tab.

4. Click [LAN Settings].

Internet Options
General Security Privacy Content Connections Programs Advanced
To set up an Internet connection, click Setup.
Setup...
Dial-up and Virtual Private Network settings
Add...
Remove
Settings...
Choose Settings if you need to configure a proxy server for a connection.
Never dial a connection
Dial whenever a network connection is not present
Always dial my default connection
Current None
Set Default
Local Area Network (LAN) settings
LAN Settings do not apply to dial-up connections. Choose Settings above for dial-up settings.
LAN Settings...
OK Cancel Apply

5. See the Use a proxy server for your LAN check box in the Local Area Network (LAN) Settings dialog box.

- If the check box is checked, uncheck it and click [OK].
- If the check box is unchecked, click [Cancel] and complete settings.


Local Area Network (LAN) Settings
Automatic configuration
Automatic configuration may override manual settings. To ensure the use of manual settings, disable automatic configuration.
Automatically detect settings
Use automatic configuration script
Address
Proxy server
Use a proxy server for your LAN (These settings will not apply to dial-up or VPN connections).
Address: Port: Advanced...
Bypass proxy server for local addresses
OK Cancel
Confirm that this box is not checked.

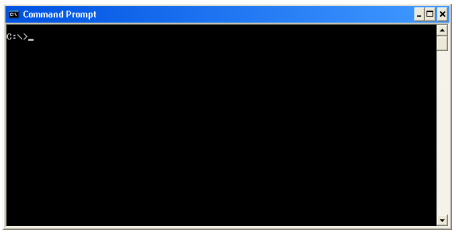
4.7 Checking the PC's IP Address and MAC Address

When this product's setup page cannot be accessed by a PC, or when data cannot not be sent/ received to/from other PCs on the network, there could be a problem with the PC's IP address settings. Take the following steps to check the IP address settings.

4.7.1 Using Windows XP/2000

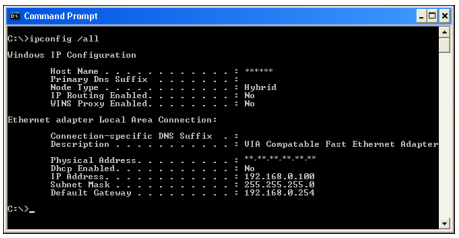
1. From the Start menu, select All programs, Accessories and Command Prompt.

- When using Windows 2000, from the Start menu, select Programs, Accessories and Command Prompt.



2. Enter "**ipconifg/all**" after the command prompt and push the [Enter] key.

- "**ipconfig/renew**" refreshes all of the LAN cards' DHCP composition parameters.
- "**ipconfig/release**" releases all of the LAN cards' DHCP composition parameters.


Command Prompt
C:\>ipconfig /all
Windows IP Configuration
Host Name . . . . . : ******
Primary Dns Suffix . . . . . :
Node Type . . . . . : Hybrid
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No
Ethernet adapter Local Area Connection:
Connection-specific DNS Suffix . :
Description . . . . . : VIA Compatable Fast Ethernet Adapter
Physical Address. . . . . : **-**-**-**-**-**
Dhcp Enabled. . . . . : No
IP Address. . . . . : 192.168.0.100
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.0.254
C:\>_

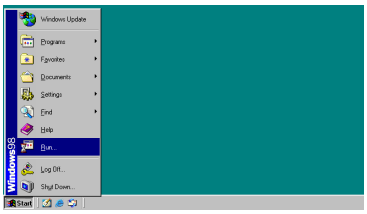
Note

The ipconfig command explanations are displayed by entering "ipconifg/?" after the command prompt.

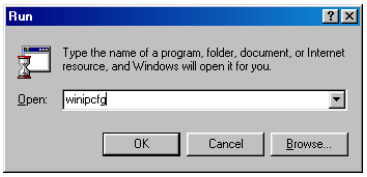
4.7.2 Using Windows Me/98SE

The following steps are for Windows 98SE.

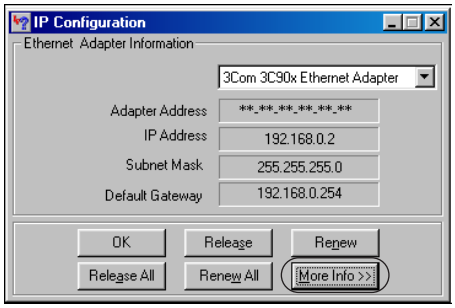
1. From the Start menu select Run.



2. Enter "**winipcfg**" in the name field and click [OK].

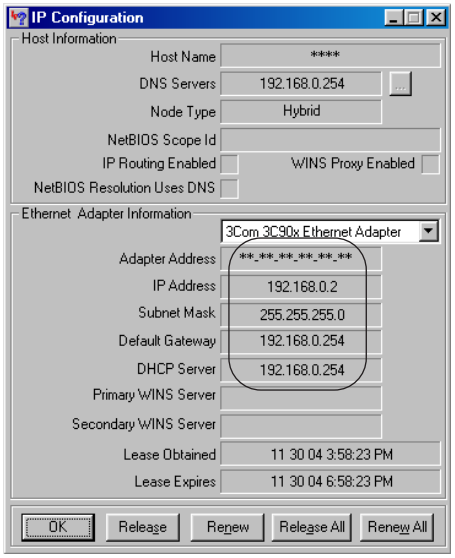


3. Select the LAN card (Ethernet adapter) with the IP address you want to check.



4. Click [More Info].

- See the IP Address field and check the set IP address.
- See the Adapter Address field and check the LAN card (Ethernet adaptor) MAC address.



Note

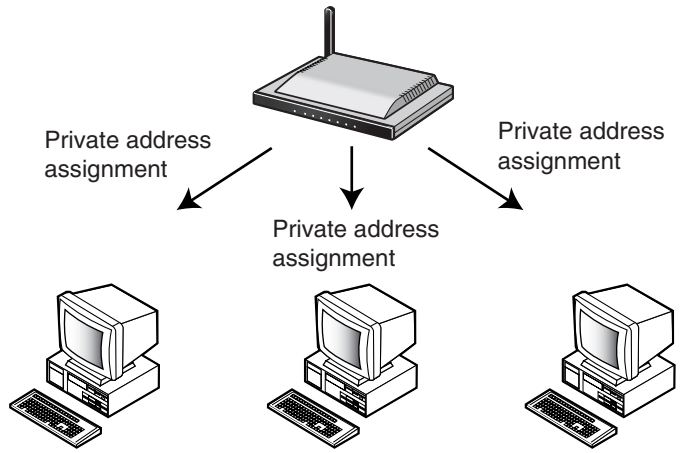
When Obtain an IP address automatically is set and a value such as 169.254.XXX.X is displayed, it is possible that the IP address was not obtained correctly. In that case, take the following steps to refresh the IP address.

1. Click [Release].
   - The automatically obtained IP address is released.
2. Click [Rewrite].
   - A new IP address is assigned.
3. Click [OK].

4.8 Stabilizing the PC's IP Address

It is necessary to set a unique IP address for each of the PCs on this product's TCP/IP network. This product can automatically assign an IP address to each of the PCs on the LAN (Home) side using the DHCP server function (factory default setting). In this case, for this product to assign and re-assign IP addresses to each PC, the PCs' IP addresses cannot be fixed.

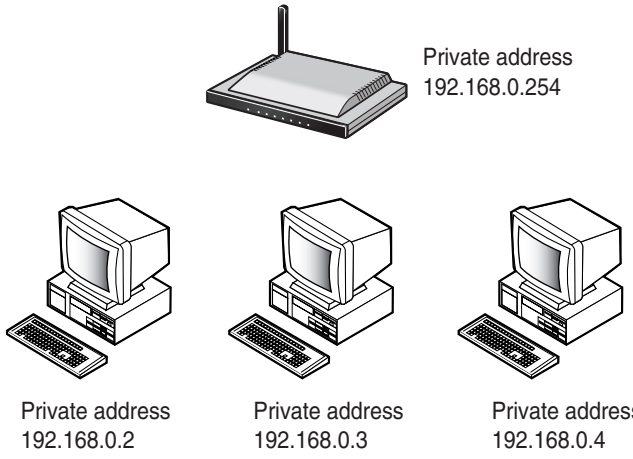
This product's IP address assignment network (factory default setting)



At the same time, it is possible to disable this product's DHCP server function, and fix each LAN side PC's private address. In this case, it is necessary to set a unique IP address to each PC in advance.

Network with stable IP addresses (Options)

This function allows you to fix a private address on the network without using the DHCP server function. It is necessary to fix a unique private address on each PC. After setting the unique private addresses, you can set this product. See page 77, and disable the DHCP server function on the options page. Follow the steps on page 132 - 133 to setup each PC.

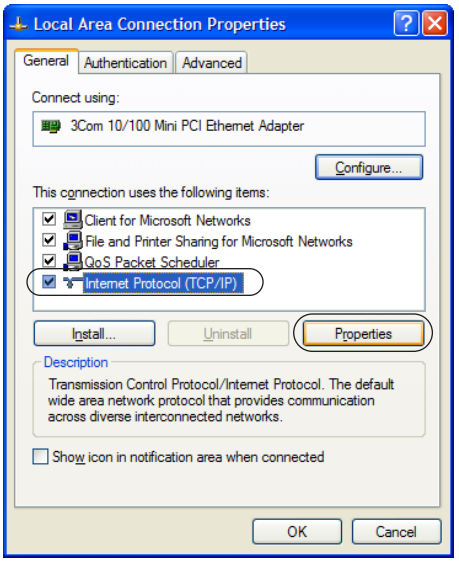


4.8.1 Using Windows XP/2000

1. From the Start menu, select My Computer, My Network, and then Display Network Connection.
   - Right-click the My Network Places icon and select Properties when using Windows 2000.

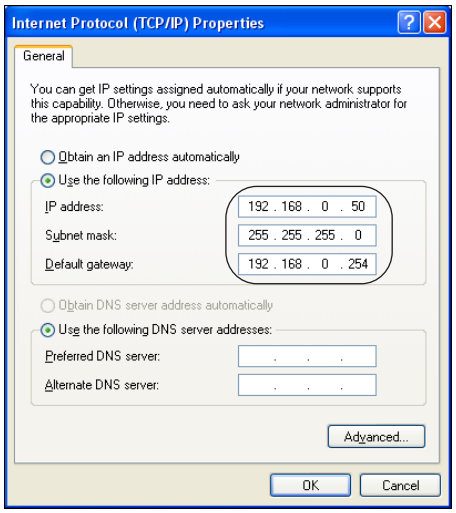
2. Right-click the icon Local Area Connection... connected to this product, and select [Properties].

3. Select Internet Protocol (TCP/IP) and click [Properties].



4. Select Use the following IP address.

5. Enter the IP address (e.g. "**192.168.0.50**") and subnet mask for each PC, and enter "**192.168.0.254**" (this product's factory default IP address) into the Default gateway field.
   - The subnet mask is usually entered as "**255.255.255.0**". To access this product's setup page, enter the same subnet mask as this product.


Internet Protocol (TCP/IP) Properties
General
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address:
192 . 168 . 0 . 50
Subnet mask:
255 . 255 . 255 . 0
Default gateway:
192 . 168 . 0 . 254
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:
Advanced...
OK
Cancel

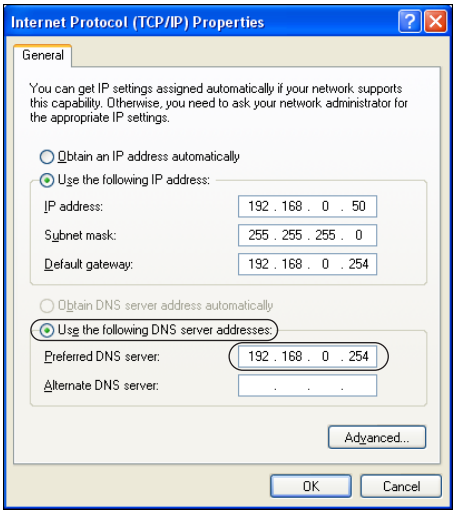
6. Click Use the following DNS server address.

7. Enter the DNS server address into the data entry field and click [OK].

8. Click [OK],

9. Close the Network Connection window and restart the PC.

- Close the Network and Dialup Connections window and restart the PC when using Windows 2000.

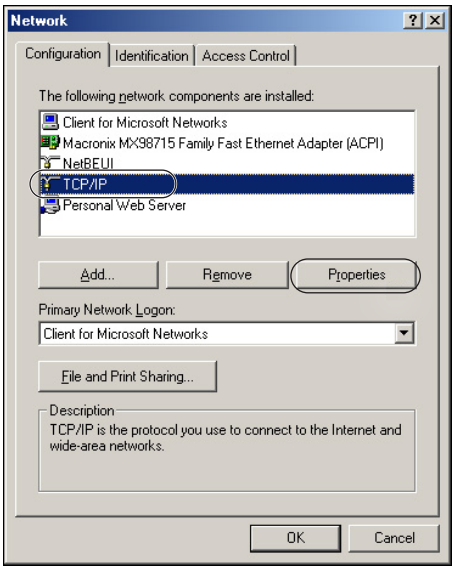

Internet Protocol (TCP/IP) Properties
General
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address: 192 . 168 . 0 . 50
Subnet mask: 255 . 255 . 255 . 0
Default gateway: 192 . 168 . 0 . 254
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server: 192 . 168 . 0 . 254
Alternate DNS server:
Advanced...
OK
Cancel

4.8.2 Using Windows Me/98SE

1. From the Start menu, select Settings and click Control Panel.

2. Double click the Network icon.

- If you cannot find the Network icon on Windows Me, click Display all Control Panel Options.



3. Select the TCP/IP related to the LAN card connected to this product in the Network dialog box, and click [Properties].

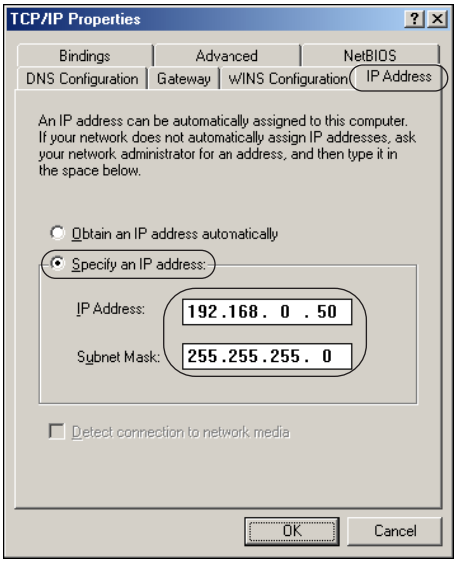
- The TCP/IP Properties dialog box is displayed.

4. Click the IP Address tab in the TCP/IP Properties dialog box.

5. Select Specify IP Address.

6. Enter the IP address (e.g. "**192.168.0.50**") and subnet mask for each PC.

- The subnet mask is usually entered as "**255.255.255.0**". To access this product's setup page, enter the same subnet mask as this product.

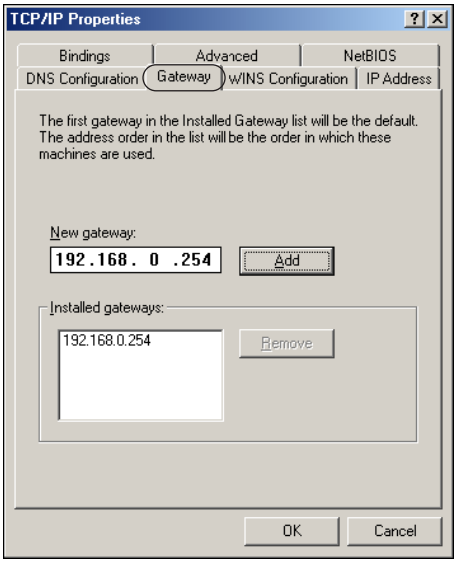

TCP/IP Properties
Bindings
Advanced
NetBIOS
DNS Configuration
Gateway
WINS Configuration
IP Address
An IP address can be automatically assigned to this computer. If your network does not automatically assign IP addresses, ask your network administrator for an address, and then type it in the space below.
Obtain an IP address automatically
Specify an IP address:
IP Address:
192.168. 0 . 50
Subnet Mask:
255.255.255. 0
Detect connection to network media
OK
Cancel

7. Click the Gateway tab.

8. Enter "**192.168.0.254**" (this product's factory default IP address) into the New Gateway address field, and click [Add].

9. Check that 192.168.0.254 is entered into the address field of Installed Gateway.

- When modifying this product's IP address, also modify the Installed Gateway address.

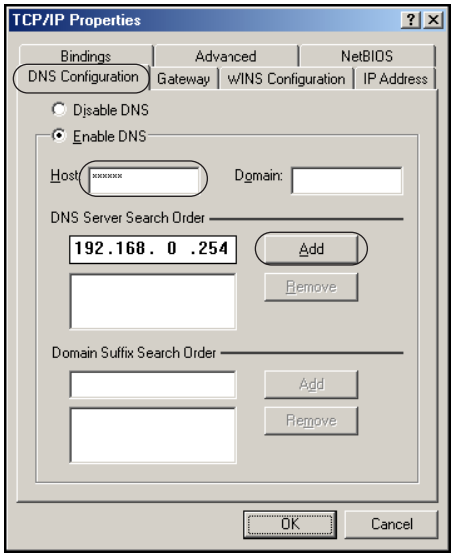


10. Click the DNS Configuration tab.

11. Select Enable DNS.

12. Enter the DNS server address into the DNS Server Search Order address field, and click [Add].

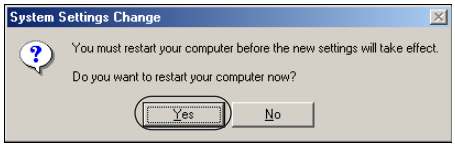
13. Enter the optional host name and click [OK].



14. Click [OK].

- The Modify System Setup dialog box is displayed.

15. Click [Yes] and restart the PC.


System Settings Change
You must restart your computer before the new settings will take effect.
Do you want to restart your computer now?
Yes
No

4.9 Factory Default Settings List

ISP Registration

ISP Registration List	No. 1	DHCP Connection
	No. 2	Unregistered
	No. 3	Unregistered
	No. 4	Unregistered

IPv6 ISP Registration

IPv6 ISP Registration List	No. 1	Unregistered
	No. 2	Unregistered
	No. 3	Unregistered
	No. 4	Unregistered

Connection Mode

Internet Connection Mode	DHCP/Static
ISP Selection	DHCP

Camera

Automatic Setup	
Automatic Setup	Enable
Available Address Range	192.168.0.151 - 192.168.0.166
Camera Port Number Setup	Specify Range
Available Port Range	60001 - 60016
IPv6 Port	80
Screen Assignment	
Camera portal page display	Camera Name and Still Image (refreshing)

Wireless

Basic	
Wireless Network	802.11b/g
SSID	(Displayed on the rear of this product)
Stealth SSID	Enable (connection through the ANY key can be denied)
Channel	7

Encryption	
Encryption Settings	WEP (WEP key is displayed on the rear of this product)
MAC Address Filtering	Disable

DynamicDNS

DynamicDNS Selection	Disable
DynamicDNS Server URL	Unset
User Name	Unset
Password	Unset
Renewal Interval	10 min

Address Translation

Basic	
DHCP/Static	Enable
PPPoE	Enable
Port Forwarding	
DMZ function	Unset

Security

Security	
Easy Security Settings	• Access by private IP addresses are rejected in both directions. (Log Output) • Access by NetBIOS/File sharing/Printer sharing/PC remote access are rejected in both directions. (Log Output)
Access Control	
Setup pages	• Restricted Access (Log Output)
Camera Portal	• None (Log Output)
Stealth Mode	• Stealth Mode can hide this product from WAN (Internet). (Regard Ident packet as an exception.) (Log Output)
Intrusion Detection	• Stateful packet inspection (Dynamic packet filtering) is enabled. (Log Output)
Packet Filtering	
Current Status	Unset

IPv6 Security

Security	
IPv6 Easy Security Settings	• Access by Direct Hosting of SMB is rejected in both directions. (Log Output) • Access by port used by RPC is rejected in both directions. (Log Output) • Communication using global addresses other than the allocated global address is forbidden. (Log Output)
IPv6 Stealth Mode	• Stealth Mode can hide this product from WAN(Internet) side IPv6 network. (Regard Ident packet as an exception). (Log Output)
IPv6 Intrusion Detection	• IPv6 Stateful packet inspection(Dynamic packet filtering) is enabled. (Log Output)
IPv6 Packet Filtering	
Current Status	Unset

Options

LAN IP Address Setting	
LAN IP Address	192.168.0.254
Subnet Mask	255.255.255.0
Port No. of Setup pages	8080
Port No. of Camera Portal	80
DHCP Server	
DHCP Server	Enable
Available Address Range	192.168.0.1 - 192.168.0.32
Static DHCP	Unset
PPPoE	
PPPoE Setting	Always
DNS Relay	Enable
MTU Size	1500 bytes (DHCP/Static) 1492 bytes (PPPoE)
Routing	
LAN	Disable
WAN	Disable
Static Routing	Unset

UPnP	
IGD	Enable
CP	Enable
Automatic deletion of UPnP port mapping (IGD)	
Timer	Indefinite
Time Setup for UPnP Port Open Request (CP)	Request a Specified Time or Indefinite

IPv6 Options

IPv6 Address (LAN)	fe80::254
RA (Router Advertisement)	Enable
Link MTU size	1500 bytes
IPv6 Dynamic Routing	
WAN	Disable
LAN	Disable
IPv6 Static Routing	Unset

VPN (PPTP)

Basic	
PPTP Server Settings	Disable
Available Address Range	192.168.0.100 - 192.168.0.103
User Registration	Unset
Options	
Authentication	MS-CHAP or MS-CHAPv2 are used
Encryption	MPPE 40 bit or MPPE 128 bit are permitted

VPN (IPsec)

IPsec	Disable
Security Policy Database Registration	Unset

Applications

Application list	Camera Status Notification application Cell Phone Camera Portal application

Password

Setup Pages	Set when accessing this product for the first time.
Camera Portal	Unset

4.10 Specifications

Main Unit

Heading	Specifications	
Power Supply	Special AC Adaptor: (Part Number: PQLV202Y)	INPUT: AC 120 V, 60 Hz OUTPUT: DC 12 V, 750 mA
Power Consumption	Maximum: About 6 W	
Dimensions (Width × Height × Depth)	About 204 mm (8.0 inches) × About 36 mm (1.4 inches) × About 140 mm (5.5 inches) (when the antenna is stored)	
Weight	330 g (0.7 lb)	
Environmental Requirements	Temperature (°C): Humidity (%):	0 - 40 (32 - 104 °F) 20 - 85 (non-condensing)
WAN Interface	Number of Ports: Connector Shape: Physical Interface:	1 8 pin modular jack (RJ-45) IEEE 802.3 (10Base-T) IEEE 802.3u (100Base-TX)
	Throughput between WAN and LAN using IPv4 (value measured at Panasonic):	Maximum of 98 Mbps (IPv4/SmartBits) Maximum of 93 Mbps (FTP [Static]) Maximum of 92 Mbps (FTP [PPPoE]) Maximum of 16 Mbps (FTP [PPTP]) Maximum of 45 Mbps (IPsec, No Encryption, SHA-1 Authentication Algorithm)
	Throughput between WAN and LAN using IPv6 (value measured at Panasonic):	Maximum of 98 Mbps (IPv6/SmartBits) Maximum of 85 Mbps (FTP [Static]) Maximum of 47 Mbps (IPsec, No Encryption, SHA-1 Authentication Algorithm)
LAN Interface	Number of Ports: Connector Shape: Physical Interface:	4 8 pin modular jack (RJ-45) IEEE 802.3 (10Base-T) IEEE 802.3u (100Base-TX)
Wireless Interface	Wireless Chip:	made by Atheros Communications

Heading	Specifications	
Wireless Interface	**IEEE 802.11b**	
	Transmission Method:	DS-SS, half-duplex
	Transmission Speed ([Standard value]Mbps):	11/5.5/2/1* (complying to IEEE 802.11b): automatic fallback
	Frequency Range (MHz):	2412 - 2462 (center frequency)
	Number of Channels:	11
	Security:	WPA-PSK (TKIP), WPA2-PSK (AES), WEP (64 bit/128 bit/152 bit), SSID, stealth SSID (hidden SSID, permitting/ not permitting connection using the ANY key), MAC address filtering
	IEEE 802.11g	
	Transmission Method:	OFDM (complying to IEEE 802.11g), DS-SS (compatible with IEEE 802.11b), half-duplex
	Transmission Speed ([Standard value]Mbps):	54/48/36/24/18/12/9/6* (complying to IEEE 802.11g): automatic fallback
	Frequency Range (MHz):	2412 - 2462 (center frequency)
	Number of Channels:	11
	Security:	WPA-PSK (TKIP), WPA2-PSK (AES), WEP (64 bit/128 bit/152 bit), SSID, stealth SSID (hidden SSID, permitting/ not permitting connection using the ANY key), MAC address filtering
	* The figures shown are theoretical maximums and not the actual figures when using the product.	
User Interface	FACTORY DEFAULT RESET button:	Returns the product to factory default settings.
	Status Indicators	
	POWER:	Displays the power/main unit status
	WAN:	Displays the WAN link status
	PPP:	Displays the PPP link status
	LAN1-LAN4:	Displays the Ethernet link status
	WIRELESS:	Displays the wireless link status

Software

Heading	Specifications	
Router Function	WAN Side Connection Mode:	IPv4: PPPoE/DHCP/Static IPv6: Tunneling/6to4/Static v6
	PPPoE Connection:	Always/Manual
	RIP:	Yes (RIPv2)
	RIPng:	Yes
	DHCP Server:	Yes (128 client setup is possible)
	DNS Relay (DNS proxy answering):	Yes
	IP Packet Filtering:	Yes (64 setup)
	Address Translation Method:	IP masquerade, port forwarding
Access Control	ID/Password	
Web Browser Setup	Yes	
Firmware Update	Yes	
VPN	PPTP Server (IPv4) IPsec (IPv4/IPv6)	

Index

Numerics
6to4 Connection 33

A
Address Translation 60
Applications 98

C
Camera 40, 42
Camera Portal 17
Connection Mode 38

D
Data Channel 48, 51
DC IN Jack 9
DHCP Connection 25
DHCP Server 77
DMZ 65
DNS Relay 80
DynamicDNS 56
Dynamic Routing 81, 86

E
Encryption 51, 54, 89, 94, 96

F
Factory Default 105, 117
FACTORY DEFAULT RESET Button 9, 117
Factory Default Settings 140
Filtering Log 112

H
Help 116

I
Indicators 9, 10
Internet Connection 37
IP Address 22, 30, 77, 132, 135
IPsec 90, 107
IPv6 16, 30, 72, 85, 124
ISP Registration 22, 30

L
LAN Jacks 9
Link MTU size 86
Logs 112

M
MAC Address Filtering 55
MAC Clone 84
MS-CHAP 89
MS-CHAPv2 89
MTU Size 80

O
Options 77, 85

P
Packet Filtering 69, 74
Password 101
Ping 108
Port Forwarding 61
PPPoE Connection 23, 79, 106
PPTP 88, 128
Proxy Server 131

R
RA 85
Restart 105, 117
Routing 81, 86

S
Save Settings 104
Security 66, 72
Setup 13
Specifications 145
SSID 48, 50
Stateful packet inspection 67, 73
Static Connection 27
Static DHCP 78
Static v6 Connection 35
Status 109
Straight cable 8
Support 116

T
Top Page 11
Tunneling Connection 31

U
Update Firmware 102
UPnP™ 82, 119

V
VPN 88, 90, 107

W
WAN Jack 9
Wireless 48

For product service

- Panasonic Servicenters are listed in the servicenter directory.
- Call 1-800-272-7033 for the location of an authorized servicenter.
- This product is designed for use in the United States of America. Sale or use of this product in other countries/areas may violate local laws.

When you ship the product

- Carefully pack your unit, preferably in the original carton.
- Attach a letter, detailing the problem, to the outside of the carton.

  Symptom

  _____

  _____
- Send the unit to an authorized servicenter, prepaid and adequately insured.
- Do not send your unit to the Panasonic Consumer Electronics Company listed below or to executive or regional sales offices. These locations do not repair consumer products.

The information in this document is subject to change without notice.

Panasonic Consumer Electronics Company,
Division of Panasonic Corporation of North America
One Panasonic Way,
Secaucus, New Jersey 07094

Panasonic Puerto Rico, Inc.
San Gabriel Industrial Park, Ave. 65 de Infantería, Km. 9.5,
Carolina, Puerto Rico 00985

Copyright:
This material is copyrighted by Panasonic Communications Co., Ltd., and may be reproduced for internal use only. All other reproduction, in whole or in part, is prohibited without the written consent of Panasonic Communications Co., Ltd.

© 2004 Panasonic Communications Co., Ltd. All Rights Reserved.

PSQX3566XB KK1104GJ3056